개인정보보호 및 ID관리

1. 개요

1.1. 추진경과 및 중점 추진방향

• 추진경과

- ID(Identity)관리 및 개인정보보호 기술분야는 2007년까지의 표준화로드맵에서는 정보보호(일반)의 일부분으로 기술되었으며, 별도의 핵심기술 표준화항목으로 구성되지는 않았으나 최근 국 · 내외적으로 ID 도용에 따른 피해액이 급증하고, 국내의 경우 ID 도용이 사회적인 문제가 되고 시장에서 산업적인 요구사항이 증가함에 따라, ID관리 기술 및 개인정보보호가 정보화/지식 사회의 필수 요소로 인식되고 있음. 이에 따라, 국 · 내외적으로 개인정보보호 및 ID관리 핵심 기술의 개발이 활발히 진행되고 있으며, 이들 핵심 기술에 대한 표준화 작업이 ITU-T, ISO 등과 같은 국제 표준화 단체에서 활발히 진행되고 있음. 이러한 개인정보보호 및 ID관리 기술 개발의 가속화와 국제표준화 추세를 감안하여 Ver. 2008의 중점기술에 개인정보보호 및 ID관리 분야가 새롭게 포함되어 중장기 표준화로드맵을 수립하게 됨

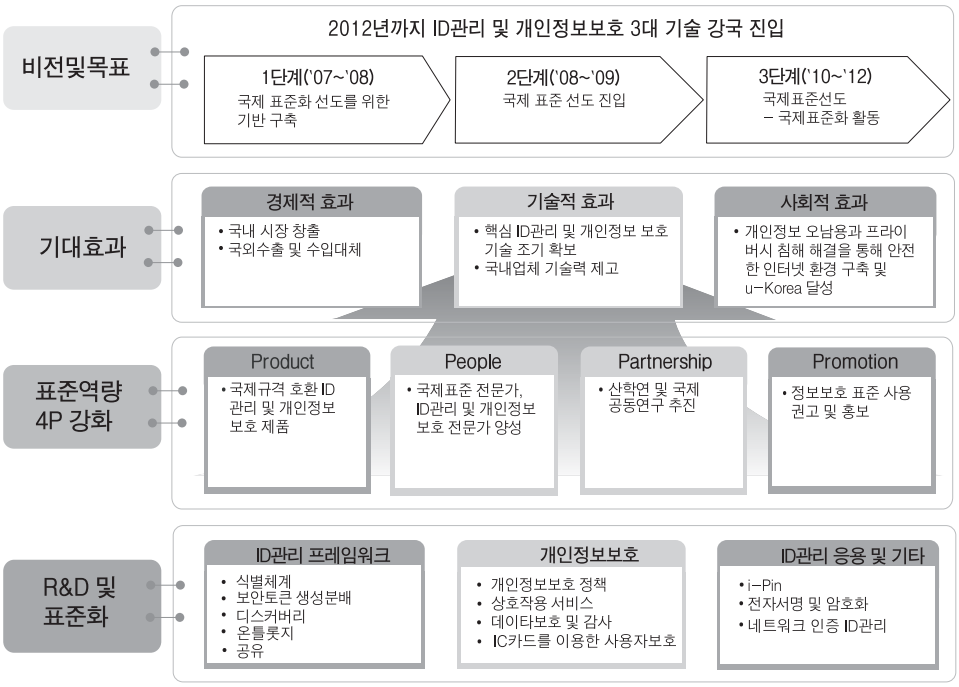
• 중점 추진방향

- 개인정보보호 및 ID관리 분야의 기술과 표준화 필요성에 대한 이해 제고를 위해 기술 개요, 국 · 내외 기술개발 동향, 국 · 내외 시장 동향 및 표준화 동향을 기술함
- 정부의 정책 추진 의지, 산업체의 요구사항, 적시성, 시장파급성, 국제경쟁력, 상용화 가능성과 같은 전략적 중요도와 타 기술에 대한 파급효과, 산업적 파급효과, 미래 영향력 등과 같은 기술적 파급효과를 고려하여 개인정보보호 및 ID관리 분야의 중점 표준화 항목을 선정함
- 국 · 내외 기술/시장/표준화 동향을 고려하여 중점 표준화별 세부전략을 수립하고 중장기 표준화 로드맵을 작성함

1.2. 표준화의 Vision 및 기대효과

• 2012년까지 국내 개인정보보호 및 ID관리 기술력이 세계 3대 기술 강국으로 진입하는 것을 목표로 국제표준화를 추진함으로써,

- 국내 우수기술의 국제표준화 선점 및 국내산업 기술경쟁력 강화
- 개인정보보호 및 ID관리 분야의 시장 창출, 국외수출 및 수입대체를 통한 개인정보보호 및 ID관리 산업 진흥
- 개인정보 오 · 남용과 프라이버시 침해 해결을 통해 안전한 인터넷 환경구축 및 u-Korea 달성



〈그림 1〉 개인정보보호 및 ID관리 기술 표준화 비전 및 기대효과

- 개인정보보호 및 ID관리 기술의 경제적 효과
  - 국내의 경우, 전체 ID관리 시장이 2005년도 246억 원으로 추정되고 있으며, 2006년부터 2010년까지 연평균 성장률은 12%로 급성장하여 2009년에는 425억 원에 이를 것으로 전망하고 있음
  - 전세계적으로 ID관리 및 접근 권한 관리의 시장 규모를 2006년 현재 30억 달러에서 2001년에 49억 달러에 이를 것으로 IDC는 전망하고 있음
  - 2007년도 한국정보보호진흥원 조사에 의하면, 국내의 경우 인터넷 이용자들이 느끼는 연간 개인정보보호에 대한 총 가치는 약 1조 2,982억 원에 달하고 있음

- ID관리 프레임워크, 개인정보보호 및 ID관리 응용 등과 같은 개인정보보호 및 ID관리 분야의 핵심 기술을 개발하고 이들 기술에 대한 국내표준을 개발하고, 우수기술에 대해 ITU-T와 ISO/IEC JTC1 등 국제표준화 단체의 국제표준 채택을 추진함으로써,
  - ID 도용으로 발생하는 막대한 경제적 피해와 피싱(Phishing) 등과 같은 개인정보보호 유출 문제를 방지할 것을 기대함
  - 시스템적 시각에 의한 빅브라더 가능성에 대한 사용자 개개인이 스스로 자신의 정보를 지킬 수 있는 기반 제공을 기대함

- 국제 표준화된 우수 기술을 탑재한 국내 개인정보보호 및 ID관리 관련 제품의 출시를 통해, 국내 관련 분야의 시장을 창출하고, 해외수출 및 수입대체 효과를 기대함
- 활발한 국제 표준화 활동을 통해, 관련 기술에 대한 다수의 IPR 확보를 기대함
- 일반 인터넷 사용자의 개인정보 오 · 남용에 대한 우려를 해결하고, 편리한 ID관리 기술을 제공함으로써, 안전한 인터넷 환경을 구축하여 u-Korea 구축의 초석을 다짐

• 개방과 공유를 특징으로 하는 웹 2.0 환경 및 서비스 확대에 따라 지금까지 개인정보의 활용과 관리를 정부기관이나 기업에 맡겼던 개인정보 소유자들이 ID관리 시스템간 상호호환을 통해 개인정보 중복성 최소화 및 자기정보 통제권 실행을 통해 다양한 통신환경에서 개인화된 서비스 활용이 가능할 것임

• "인증 프레임워크와 ID관리 프레임워크의 통합 적용 및 운영", "NGN의 이종 액세스를 통합하는 접속 보안 인증 및 액세스 인증 ID관리"등 기술을 표준화된 방법으로 구현하게 되면, 사용자들은 다양한 통신망 서비스에 접속하면서 여러 가지 종류의 ID 사용으로 인한 불편과 정보 노출 위험성에서 보호되며, 안전한 통신 접속 환경이 보장되어 새로운 서비스를 위한 보안 조치 및 추가 비용 부담이 배제된 각종의 새로운 통신 서비스 제공이 가능해 질 것임. 통신 서비스를 제공하는 사업자의 입장에서는 통신 시스템의 도용 위협으로부터 자유로워지고, 새로운 서비스 시스템의 도입을 위한 보안 조치 비용 부담이 절감되므로, 이로 인한 비용 절감을 사용자와 공유할 수 있게 될 것임

• 세계 최고수준의 초고속통신망과 3G 통신망 인프라가 결합된 우리나라의 앞선 IT환경에서 표준화된 ID관리 시스템 개발과 적용을 통해 프라이버시가 보호되면서 유비쿼터스 서비스가 제공되는 모범사례 구축 및 실생활 활용이 가능함

1.2.1. 표준화의 필요성

• 인터넷의 활용이 커져가면서 사용자는 수많은 사이트에 ID를 등록하게 되고 자신의 개인정보를 여러 곳에 방치하게 됨으로써 ID관리의 불편함뿐만 아니라 개인정보 오 · 남용으로 인한 피해가 증가하고 있음
- 일반 인터넷 이용자들이 느끼는 연간 개인정보보호에 대한 총 가치는 약 1조 2,982억 원에 달하고, 개인정보 중에서 특히 금융정보 유출을 가장 우려하고 있는 것으로 나타남
  ◦ 한국정보보호진흥원, "정보통신부 보도자료," 2007.1
- 사용자의 ID 수가 증가하고 개인정보 공유에 대한 요구가 증가함에 따라, ID관리의 불편함뿐만 아니라 개인정보 오 · 남용으로 인한 피해가 증가하고 있음
  ◦ MIC & KISA, "u-정보보호 마스터플랜," 2006.10
  ◦ OECD WPISP, "Background paper on digital identity management," 2006.10

- NGN/BcN은 통신망에 인터넷 기술의 특성을 추가하고 있어 사용자가 임의의 접속점을 통해 망에 접속하는 것이 가능함에 따라 사용자 로그인 및 인증절차가 필수적으로 요구되며, 관련 ID들을 적절하고 안전하게 관리하는 표준화된 방법을 정의하는 것이 NGN/BcN의 상용화 도입을 위해 필수적임
  - 인증을 위한 개인의 ID는 NGN/BcN 망 내에서는 다양한 망 요소들 간의 ID 및 프로파일의 형태로 전환되어 존재하게 되는데, 이들 ID의 생성과 소멸 등 생명주기(Life Cycle)가 적절히 관리되지 않고 망 내에 방치될 경우, 혹은 이들 ID들이 적절히 보호되지 않고 제 3자에 의해 탈취 가능한 상태에 놓일 경우, 해당 사용자 및 통신망은 도용 등 금전적인 문제를 포함한 각종 위협에 놓이게 되며, 이러한 위협은 궁극적으로 NGN/BcN의 상용화 서비스 자체를 불가능하게 할 수 있음

- 최근 전자여권, 전자운전면허증과 같은 국제적 표준 IC카드의 등장과 전자주민증(주민등록 발전모델)과 같은 개인 신원증명(ID)이 IC카드로 발급되고 있으나, 각 ID를 발급하는 기관의 안전성 보장 외에 IC카드를 발급받아 사용하는 일반 사용자에 대한 개인정보 보호 방안을 체계적으로 연구할 필요가 있음

- 이와 같은 문제를 해결하기 위해, 국내에서도 개인정보보호 및 ID관리 핵심 기술에 대한 연구 및 개발이 진행되고 있으며 이들 기능이 탑재된 제품이 출시되고 있는 상황이지만 상호운용성을 제고하기 위한 개인정보보호 및 ID관리 제품에 대한 표준의 부재는 안전한 전자상거래와 전자정부 구현에 대한 장애가 되고 있으며, 나아가 NGN/BcN의 성공적인 상용화 추진에 있어 중요한 기술적 결함이 될 수 있음

- 특히 세계 각국은 자신이 개발한 기술을 국제 표준에 반영함으로써, 관련 제품에 대한 IPR(Intellectual Property Rights)을 확보하고 관련 제품의 기술경쟁력과 시장지배력을 향상시키고 있는 추세임

- 또한, 현재까지 개인정보보호 및 ID관리 분야에 대한 국내의 표준화 활동은 주로 국제 표준을 국내 실정에 맞게 개정하거나 준용하는 수준에 머물러 있음

- 따라서 개인정보보호 및 ID관리 분야의 표준화는 개인정보보호 및 ID관리 제품의 국제표준 준용 및 상호호환성(Interoperability) 제고를 통해 국내시장 창출 및 해외수입 대체 및 수출 증대를 가져올 수 있으며, 핵심 기술에 대한 국제 표준화를 통해 IPR을 확보하고 관련 제품의 기술경쟁력과 시장지배력을 향상시킬 수 있음

- 웹 기술의 보편화와 함께 웹 정보 시스템을 통한 정부 또는 기업의 대국민, 대고객 서비스가 확산되고 있으며, 개인들은 자신의 개인정보와 선호정보(preference)를 웹 정보 시스템이 활용하도록 함으로써 다른 사용자와는 차별화된 개인화된 서비스를 이용할 수 있게 됨. 현재 각 정부기관 및 기업들은 서비스 제공자 관점에서 서비스 제공에 필요한 고객의 개인정보를 각각 수집, 저장, 활용하고 있는 실정임

- 그러나 개인정보 소유자 관점에서 평가할 때 개인정보를 관리하는 현재 정보시스템 체계에서 자신의 개인정보는 각 정부기관 및 기업의 정보 시스템간 상호호환성 부재로 중복, 저장되어 있고 개인정보 활용시 개인정보 소유자에 대한 사전고지 및 동의 절차 미비 등으로 인해 개인정보의 유출 위험성과 오 · 남용으로 인한 경제적, 사회적 비용발생 문제점을 안고 있음. 이러한 문제들의 근본적인 문제는 개인정보를 수집, 저장, 공유, 관리, 활용, 폐기 서비스를 수행하는 ID관리 시스템에 대한 기능 요구사항, 프레임워크, 시스템 구현을 위한 메커니즘 개발 및 이를 지원하는 제반 법률 및 제도적 장치가 존재하지 않는데 있음

- 현재 개발되어 사용 중인 ID관리 시스템들은 각 ID관리 시스템들이 사용되는 응용분야 특성에 따라 제공되는 서비스, 서비스 구현을 위해 사용되는 프로토콜이나 메커니즘 등이 다르므로 이종 ID관리 시스템간 서비스 발견, 안전한 개인정보 공유, 상호호환이 불가능하여 결과적으로 효율적인 ID 서비스 제공과 개인정보 안전한 공유, 관리가 불가능한 문제점이 있음

1.2.2. 표준화의 목표

- 2008년까지 1단계로 ID 식별체계, i-PIN 표준 등 국내표준을 개발하여 국제 표준화 기반 구축
- 2009년까지 2단계로 개인정보보호 및 ID관리 핵심 기술을 개발하고 ITU-T, ISO 등 국제표준화 단체 기고를 통해 ID 관련 국제 표준화 선도 진입
- 2012년까지 3단계로 개발된 핵심 기술의 국내 표준화 및 우수기술에 대한 국제표준화 진행으로 국제표준화 선도

- 2008년까지 개인정보보호 및 ID관리 기술 대한 국내 기반조성을 위하여 ID 식별체계, ID 관련 용어 및 i-PIN(Internet Personal Identification Number)의 국내 표준화 완료 및 ITU-T, ISO/IEC, 3GPP(3rd Generation Partnership Project) 등 개인정보보호 및 ID관리 관련 국제 표준화 단체에 참여함으로써 국제 표준화 기반을 구축함

- 2010년까지 개인정보보호 및 ID관리 핵심 기술을 개발하고, ITU-T/SG2, SG11, SG13, SG17, ISO/IEC JCT1/SC17, SC27 등 국제 표준화 단체에 개발된 핵심 기술에 대한 표준을 기고함으로써 ID관리 분야의 국제 표준화를 선도할 수 있는 상태에 진입

- 2012년까지 국제표준화 선도를 위하여 ID관리 프레임워크, 개인정보보호 및 ID관리 응용과 기타 분야의 핵심 기술들에 관한 국제표준(안) 개발을 적극적으로 주도하여 ITU-T/SG2, SG11, SG13, SG17, ISO/IEC JTC1/SC17, SC27 등 국제표준화 기구 관련 특허를 다수 획득

- 계층구조의 통신망인 NGN/BcN 망을 위해서는, "이종 액세스 접속 통합 인증 및 액세스 ID 통합 관리기술", "서비스 계층 통합 인증 및 서비스 프로파일링 기술", "응용 계층 통합 인증 및 bootstrapping 프레임워크와 SSO 기반 ID 관리 시스템 통합" 등 표준을 개발하고, 이들을 NGN/BcN에 적용 가능한 표준으로 개발하기 위해 국 · 내외 표준화에 참여하는 것을 목표로 함. 국내에서는 통합번호체계 포럼, TTA PG 206(신호방식) 및 PG 206(NGN) 등에 참여하며, SG2, SG11, SG13 분과위원회의 협력과 지원을 받아 국제 표준화에 참여하며, 효율적인 ID관리 시스템 구축을 위해, ITU-T SG17 의 IdM Focus Group과 SG13 NGN, 그리고 3GPP SA 및 TISPAN WG3,4 그룹을 통한 국제 표준화를 추진

- 지금까지 개발된 ID관리 시스템들은 사용자중심, 응용중심, 네트워크중심 등 특정 응용분야에 한정된 제한적 기능만을 제공하고 있는 한계가 있고 ID관리 시스템간 서비스 발견, 정보체계 및 정보공유 프로토콜을 위한 표준 부재로 인해 상호호환이 불가능한 문제점을 안고 있음. 따라서 이러한 단점들의 극복을 위해 특정 응용분야에 국한되지 않는 포괄적인 ID관리 시스템 요구사항을 정리하고 현재 사용 중인 유 · 무선 통신망뿐만 아니라 미래 유비쿼터스 통신망에도 적용가능하고 다른 ID관리 시스템과 상호호환이 가능한 ID관리 시스템 아키텍처 및 모델의 개발은 필수적임

- 또한 ID관리 시스템간 상호호환성을 통해 사용자에게 최적화된 서비스 제공을 위해 개인정보 구조에 대한 표준 스키마, 개인정보의 안전한 공유를 위한 ID 공유 프로토콜, 각 ID관리 시스템에서 제공하는 서비스 표현방식 및 발견 프로토콜, ID관리 시스템에서 사용하는 인증 메커니즘 평가 척도, 그리고 ID관리 시스템이 개인정보 활용과 공유를 통해 최종 사용자에게 서비스를 제공할 수 있도록 지원하는 법률 및 제도적 장치의 정비 등이 표준화 목표임

2. 국 · 내외 현황분석

2.1. 중점기술개요

2.1.1. 중점기술 및 표준화항목의 정의

• 중점기술의 정의

ID관리 기술은 인증정보를 비롯한 개인의 특징, 신상정보, 선호도와 같은 ID의 생성부터, 변경, 유통, 폐기 등에 대한 라이프 사이클을 인터넷 및 통신망 환경에서 안전하고 통합적으로 관리하는 기술로 요약할 수 있음
ID관리 기술은 사용자의 편의성과 안전성, 개인정보보호 수준을 높이고 사업자의 관리비용 감소와 시스템 보호 및 조직 간 서비스 연계 등을 지원하는 기술이며, 차세대 웹 환경을 위한 필수 정보보호 기술 및 IP 기반의 통합망인 NGN/BcN의 상용화를 위해서도 역시 필수적인 기술임

- ID는 사이버스페이스 상에서 개인식별을 가능하게 함으로써 개인의 안녕과 이해관계에 영향을 미치는 모든 정보로서 식별자(Identifier)와 속성들(Attributes)로 구성되며, '공공기관의개인정보보호에관한법률' 제2조 2항에 정의된 개인정보[2]와 유사한 의미로 쓰일 수 있음. 또한 ID를 ITU-T에서는 엔티티를 설명하고 인식하기 위한 속성 또는 엔티티에 대해 알려진 속성들로 정의하고 있으며, Liberty Alliance와 OASIS(Organization for the Advancement of Structured Information Standards)의 SAML(Security Assertion Markup Language)에서는 엔티티가 지닌 속성들로 설명되는 엔티티의 본질로 정의하며, OpenGroup에서는 지역, 기업, 국가, 글로벌 같은 지정된 콘텍스트 내에서 객체를 유일하게 식별할 수 있는 기본 개념으로 정의하고 있음
- ID관리 기술은 차세대 웹을 위한 필수 정보보호 기술로 인식되고 있으며, 사용자 식별과 인증에 국한되어 있던 응용범위를 넘어 인터넷에 분산된 개인정보를 연계하는 매쉬업(Mash-Up) 서비스, 콘텐츠의 공유 및 사용자의 참여 그리고 개방을 통한 고부가 가치를 제공하는 웹 2.0 서비스, 행정정보공유를 통한 u-전자정부 서비스, 의료정보공유를 통해 국민건강을 증진하는 u-Health 서비스 등을 위한 높은 안전성과 개인정보보호 수준을 보장하는 기술이며, 2007년 매출이 9억 1천만 달러에서 2009년에 24억 달러 규모로 높은 성장률을 보일 것으로 예상(출처:Radicati Group, Identity Management Market 2005-2009, Sep 2005)되는 기술임
- 현재 인터넷은 단순히 정보 교환을 위한 수단이 아니라, 각종 정보의 생산, 가공, 교환 등의 행위가 이루어짐으로써 사용자들에게 다양한 서비스 및 생활 환경을 제공하고 있음. 인터넷의 활용이 커져가면서 사용자는 수많은 사이트에 ID를 등록하게 되고 자신의 개인정보를 여러 곳에 방치하게 되어 ID관리의 불편함과 남용될 수 있는 위험에

2) "개인정보"라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명.주민등록번호등의 사항에 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말함

항상 노출되어 있음. 또한 피싱, 파밍(Pharming) 공격 등과 같은 개인정보 유출로 인한 피해 사례들이 계속적으로 보고되고 있으며, 2005년 7억1천4백만달러 규모에서 2010년에는 16억 달러에 이르는 피해가 예상되고 있음 (출처:IDC, Worldwide Identity Theft Black Market 2006-2010 Forecast, Dec 2006). ID관리 기술은 이러한 현재의 인터넷이 갖고 있는 문제들을 근본적으로 해결할 수 있는 핵심 요소기술임

- ID관리 기술은 광범위한 기술들이 종합적으로 융합된 기술로서 Microsoft, SUN, Oracle 등 대부분의 IT관련 선도 업체들은 ID관리 핵심기술 개발에 많은 노력을 기울이고 있음. 또한 유럽을 비롯한 일본, 미국 등에서는 정부주도의 프로젝트에 계속적으로 투자하고 있으며, 관련기술의 주도권을 확보하고 빠른 기술보급을 위한 표준화 작업을 ISO/ITU, W3C, OASIS 등의 국제표준화 단체를 통해 추진하고 있음
- 유 · 무선, 회선과 패킷망 및 웹 기반 서비스구조 등 다양하고 이질적인 기술들을 통합하려는 NGN/BcN 망에서는 다양한 ID들의 통합 연동이 기본 이슈가 되며, 이들을 통합 관리하는 기술의 도입이 필요함. 기본적으로 다양한 단말 ID들의 통합 인증 기술이 개발되어야 하며, 이들을 효율적으로 관리하는 방법과, ID 사용의 안전성을 지원하는 SSO(Single Sign On) 기술 등을 위해 신뢰성 관리 기술이 필요함. 궁극적으로, 통신망 내에서 이들은 모두 통합된 일련의 계층구조 프레임워크로 수용되어야 하며, 단대단(End-To-End)에 일관적인 "NGN 인증 ID 및 Key 관리 구조"로 설계되어야 함

• 표준화항목의 정의

중점 표준화항목	정의	대상 표준화항목	표준화 내용
ID관리	ID 정보의 식별, 디스커버리, 의미, 형식, 공유 프로토콜 및 공통 프레임워크 기술 표준	식별체계	멀티도메인에서 식별가능한 단일 식별자의 정의 및 생성 · 관리 규격
		보안토큰 생성 · 분배	인증, 권한 및 속성 정보를 포함한 보안토큰의 생성 및 검증 규격
		디스커버리	ID 정보의 요청 · 제공, 이를 위한 ID 서비스 발견 메커니즘과 메타데이터의 질의 및 응답 프로토콜 규격
		온톨로지	시스템 간 자동화된 정보의 교환과 이용이 가능하도록 ID의 개념과 관계를 정의
		공유	ID 정보 공유를 위한 메시지 형식과 프로토콜 규격
		프레임워크	ID 생성, 저장, 유통, 관리 서비스를 위한 공통 프레임워크 규격
		신뢰 관리	통신 당사자 간의 협상을 통한 신뢰구축 메커니즘과 보안토큰 요청 · 응답 메시지 및 전송에 대한 규격
개인정보보호	개인정보정책 설정 · 협상 규격 및 개인정보 생명주기별 프라이버시 관리 모델 표준	개인정보보호 정책	개인정보 획득에 따른 의무와 이용범위 등에 대한 정책 생성, 공개, 검토를 위한 형식
		상호작용 서비스	개인정보 이용과 제공을 위해 사용자 또는 대리인의 동의를 받기 위한 상호작용 서비스 프로파일
		데이터보호 및 감사	ID 데이터 보호 프로파일 및 개인정보 이용과 제공에 대한 감사정책
		IC카드 이용 사용자 보호 기술	IC카드를 사용하는 시스템에서 IC카드에 탑재하여 사용자를 보호할 수 있는 기술
ID관리 응용 및 기타	주민번호대체 기술 및 네트워크 중심 ID 관리 기술 표준	i-PIN	주민번호 대체를 위한 서비스 프레임워크 및 서비스 전달 메시지 형식 규격
		네트워크 중심 ID관리	차세대 유레ゼ 통합 통신 시스템에서의 계층별 통합 인증을 위한 보안 프로토콜 및 인증-ID관리 통합 메커니즘 표준 규격
		XML 전자서명 및 암호화	ID 정보를 포함한 XML 문서의 암호화와 서명 바인딩 규격

- ID 식별체계 표준화는 서로 다른 도메인간에서도 사용자의 ID를 유일하게 구분 · 확인할 수 있는 식별자의 생성, 분석, 관리를 위한 규칙 등을 정의하며, URI(IRI), XRI(eXtensible Resource Identifier), OpenID 등의 최근 인터넷 표준 식별체계 기술들을 참조함. URI(Uniform Resource Identifier)는 IETF(Internet Engineering Task Force)와 W3C에 의해 제정된 웹 주소 표준으로 인터넷 자원들의 구체적 주소를 표현하는 URL(Uniform Resource Locator)과 지속성을 보장하기 위한 추상적 주소를 표현할 수 있는 URN(Uniform Resource Name)으로 구성됨. OASIS에서 표준화를 진행 중인 XRI는 추상화되고 구조화된 식별체계를 가지며 도메인, 위치, 응용 분야, 통신 프로토콜 등에 무관한 고유 식별자를 정의할 수 있는 방법을 제공하나 URI와 달리 인터넷에 추가적인 식별 시스템들을 구축해야 하는 어려움이 있음. OpenID는 하나의 URI로 인터넷 사용자를 유일하게 식별해주는 기술로 Web 2.0 환경에 적합한 기술로 보급이 확산되고 있음
- 보안토큰은 서비스요청 주체(subject)가 서비스제공 주체의 서비스 이용을 지원하기 위해, ID관리 주체가 서비스요청 주체에게 발급하고 서비스제공 주체에게 전달하는 주장정보(인증, 권한, 기타속성 정보)를 통칭하며, SAML, Kerberos, X.509 등의 기술들을 통해 생성됨. 보안토큰은 주로 단일인증 및 권한관리 기술의 일부로 사용되어 왔으나 ID관리 기술의 발전과 새로운 요구사항이 대두되면서 사용자의 ID 정보를 전달하는 매개체로 이용되는 추세임. 예를 들어, Microsoft의 CardSpace와 같은 새로운 ID 기술은 SAML 보안토큰을 기반으로 사용자의 속성정보를 전달함. 보안토큰 표준화는 Liberty Alliance의 ID-FF(IDentity Federation Framework), W3C의 WS-Security(Web Service Security), OASIS의 WS-Trust 등 기존 표준과의 상호운영을 고려하여 보안토큰의 생성, 전달, 검증, 이용에 관한 표준을 준비하고 ID 공유기술 등과 같은 새로운 기술들에 대응할 수 있는 다양한 프로파일들을 준비함
- 디스커버리는 ID 열람권한을 획득한 주체(주로 서비스제공자 시스템)가 사용자 ID를 획득하기 위해, 사용자가 제공한 ID 식별자에 기반하여 ID 정보제공자의 ID 관련 서비스 위치와 사용되는 프로토콜, 보안 메커니즘 등을 확인하는 기술이다. ID 열람 서비스를 제공하는 ID관리 주체는 외부에서 접근할 수 있는 서비스 인터페이스와 정책을 메타데이터 형태로 노출하고, 필요한 경우 서비스 요청 주체와의 협상을 통한 서비스가 가능하도록 함. 디스커버리 표준화는 서비스 위치, 프로토콜, 보안 메커니즘 등에 대한 메타데이터의 교환 프로토콜 및 메시지 포맷 등을 정의하며, YADIS, SXIP, Liberty Alliance 등의 기술을 사용하여 제공되는 디스커버리 서비스들 간의 상호운영을 위한 프로파일을 준비함
- 온톨로지는 시스템 간 자동화된 정보의 교환과 이용이 가능하도록 ID의 개념과 ID간 관계를 정의하고 관리하여 컴퓨터가 ID 관련 정보를 스스로 해석하고 처리할 수 있도록 하는 기술로, 특정 응용 도메인 또는 글로벌 도메인에서 교환되는 ID의 공통 사전 · 스키마에 대한 표준이 필요함. 또한 ID 정보 분석과 판단의 정확성을 높이기 위해 상황인식 정보(Context-Awareness) 등과의 연계를 위한 관련 표준화가 필요함
- ID 공유 표준화 항목은 동일 도메인 내에서 또는 연계된 도메인들 내에서 사용자의 정보를 주고받는 사업자 중심의 공유 기술과 사용자 정보가 해당 사용자를 거쳐 확인되어 전달되는 사용자 중심의 공유 기술을 다루고 있음. ID 공유는 개인정보를 연계하는 매쉬업 서비스 등을 제공하거나 다양한 도메인 내에 분산화된 사용자 정보의 동기화에 필수적인 기술로, ID 공유 과정에서 발생할 수 있는 프라이버시 및 보안 위험 등을 분석하고 상호운영성 문제 등을

해결하기 위한 사전 연구가 필요하다. 현재 개발되어 서비스 중이거나 개발 중인 공유 기술은 Liberty Alliance의 ID-WSF(IDentity Web Services Framework), CardSpace, XDI(XRI Data Interchange) 등이 있으나, 좀 더 발전된 형태의 서비스들이 계속적으로 등장할 것으로 예상

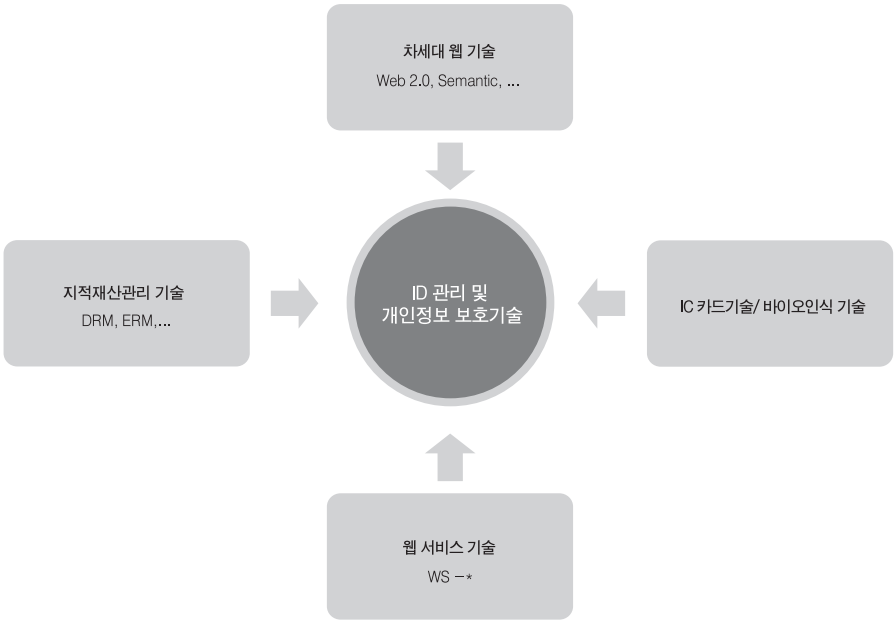
- 프레임워크 표준화는 ID의 생성, 저장, 유통, 폐기와 같은 생명주기 관리 서비스를 위한 공통의 프레임워크 규격을 정의하여, 이를 바탕으로 ID 응용 간 상호호환성 문제를 해결하고 관련 업체의 ID 응용기술 개발과 이용을 촉진함. 개발되는 표준은 ID 관련 용어 통일, 다양한 연관 표준 수용과 상호운영을 위한 아키텍처 그리고 공통 API를 포함하며, 높은 보안과 프라이버시를 위한 운영 시나리오, 프로파일 등을 마련함
- 개인정보보호정책 표준화 항목은 개인정보 획득에 따른 의무와 이용범위 등에 대한 정책 생성, 공개, 검토를 위한 형식을 마련함. 개인정보보호정책은 개인정보보호 관련 법률과 권고안에서 정한 범위를 준용하면서도 개인정보 취득자의 다양한 비즈니스 상황을 고려해 준비되어야 함. 개인정보보호정책 공개는 P3P와 같은 표준화된 기술을 사용하여 개인정보제공자가 자기정보 제공 시에 취득자의 의무와 이용범위 등을 폭넓게 인식하고 제공여부를 결정할 수 있는 방법이 제공되어야 하며, 이를 위해 개인정보제공자의 시스템에서 개인정보제공자를 대신하여 공개 정책을 분석하고 평가하여 사용자에게 보고할 수 있는 에이전트의 기능과 사용자 상호작용 메커니즘 등을 정의하여야 함
- 상호작용 서비스는 개인정보획득자(서비스제공자)가 개인정보의 이용과 제공에 대한 사용자 선호도를 사용자 별로 수집 · 관리하거나 사용자의 사전 선호도 조사로 결정될 수 없는 범위에서는 개인정보 이용과 제공 시마다 사용자와의 상호작용으로 사용자 동의를 획득하기 위한 서비스임. 예를 들어 Liberty Alliance의 ID-WSF IS(Interaction Service)와 같은 명세는 웹서비스 제공자가 웹서비스 소비자에게 서비스 제공에 필수적인 소비자 정보를 해당 소비자의 ID관리 서비스로부터 획득하는 방법 및 ID관리 서비스가 요청된 정보를 전달하기에 앞서 소비자에게 동의를 얻는 메커니즘을 설명하고 있음. 상호작용 서비스 표준화는 상호작용 서비스를 제공하기 위해 필요한 공통의 스키마와 프로파일 등을 작성함
- 데이터보호 및 감사 표준화는 ID 데이터 보호 프로파일 및 개인정보 이용과 제공에 대한 감사정책 가이드라인을 마련함. 데이터보호 가이드라인은 ID 데이터를 중요성 · 위험성별 카테고리로 구분하고, 카테고리별 사용되어야하는 암호화 알고리즘과 키 크기 및 저장방법 등에 대한 권고안을 마련함. 감사정책 가이드라인은 ID 데이터의 이용과 제공시 저장되어야 하는 감사 항목, 감사 데이터 포맷, 감사 데이터 관리 주체 등을 정의함
- IC카드를 이용한 사용자 보호 기술은 단지 시스템 접근 권한을 수여하고 개인을 인증하는 수단으로 활용되는 IC카드를 시스템의 불법적 접근으로부터 사용자의 중요 정보를 보호하는 기술의 규격을 제정하고자 하는 것임. 이를 통하여, 전자주민증 등의 정보 집중화에 의한 빅브라더 논쟁을 종식시키고 IC카드형 전자주민증 등의 도입 확산을 통하여 행정의 효율화는 기하면서 개인의 중요정보를 보호하고자 하는 것으로, IC카드 수록 개인정보 항목, 각 항목별 중요도 산정, 시스템에서의 접근시 대응 방법 및 상호인증, 중요 정보 접근시 유 · 무선 환경을 이용한 이용자 동의 요청 방법 그리고 시스템의 주요 정보 접근 기록의 유지 등을 정의함
- 신뢰관리는 통신 당사자 간의 협상을 통한 신뢰구축 방법과 보안토큰의 발급 요청 · 응답 프로토콜에 관한 것으로, 통신에 참여하는 참여자가 메시지를 교환하기 이전에 보안토큰의 종류, 보안 알고리즘, 키 정보, 메시지 포맷 등의 메타데이터를 교환하여 신뢰관계를 구축하는 메커니즘 등을 다룸. 이와 관련된 기술은 WS-Trust 등이 있으며,

Microsoft의 CardSpace와 같은 ID 서비스는 이 기술에 기반을 둠

- 네트워크 중심 ID 관리는 통신망에서 운용되는 ID 들을 통신망 사업자 혹은 설계자의 입장에서 관리하는 기술을 정의하며, 현재 ITU-T 에서 개발 중인 차세대 통신망구조 표준에 ID 관리 기술을 접합시키기 위한 제반 작업들로 구성됨. 이는 현재 ITU-T 의 Focus Group of Id Management 가 정의한 내용에 따라 네트워크중심 ID 관리 프레임워크를 비롯, 액세스/트랜스 포트계층에 대한 인증 ID 관리 기술로 대변되며, 주로 NACF (Network Attachment Control Function)에서 운영되는 기능들로 정의되어, 이종 액세스들을 통한 망 접속 시 통합 ID 인증을 위한프로토콜 및 프로파일 운영 방식, Id 의 등록, 바인딩, 신뢰 관계, 위치 정보관리등을 위한 추가적인 기능들의 설계 구현방법을 정의하게 됨. 응용 및 서비스 중심 ID 관리 기술은 통신망의 응용 및 서비스계층에서 ID 관리를 위한 주소, 번호관련 정보의 운용관리를 위한 프로파일과 policy 의 적용 방식등 기능을 설계 구현하는 표준 기술로 개발됨
- 아울러, 차세대 통신망의 응용 서비스 계층에는 인증 ID 관리 기능과 안전하고 편리한 ID 관리 매커니즘을 통합 구성해야 하는데, 이는 3GPP에서 만들어진 GAA(Generic Authentication Architecture)와GBA(Generic Bootstrapping Architecture) 표준이 정의하는 모바일환경에서의 클라이언트와 서버간의 상호인증 방식을 주로 참조함. GAA는 공유키 또는 인증서를 기반으로 상호인증을 수행할 수 있는 공통 아키텍처이며, 특히 GBA는 공유키를 생성하여 단말과 서버 간에 이를 공유하고, 이후 인증용도로 공유키를 사용할 수 있는 응용 독립적인 메커니즘을 규정함. 이러한 안전한 상호인증 메커니즘을 통신망에도 적용하여 IP 망을 기반으로 도입되는 다양한 응용이 안전한 인증프레임워크 상에서 동작하도록 하면서, 동시에 동일하고 일관된 ID 관리 매커니즘을 사용할 수있도록, Liberty Alliance 의 ID-FF 등 single-sign-on 기술 구조를 도입하여 인증과 ID 관리가 통합되는 구조와 시나리오를 작성하는 작업이 필요함
- i-PIN은 웹사이트에 주민등록번호 대신 이용할 수 있는 사이버 신원확인번호로서 인터넷 상에서 주민등록번호가 무단으로 유출되어 도용되는 부작용을 막기 위한 서비스이며, 현재 국내 인터넷 서비스 환경에서 실명확인 또는 연령확인(성인인증)시에 입력되는 주민등록번호의 과도한 사용을 줄이기 위해 정부주도 하에 개발된 기술임. i-PIN 표준화 항목은 차세대 주민번호 대체 서비스 프레임워크 및 서비스 전달 메시지 형식 규격을 마련하기 위한 것임
- ID 정보를 전송하기 위한 대부분의 메시지 포맷은 확장가능하면서 유연한 구조를 제공하는 XML 문서에 기반하며, 이러한 문서의 위변조 방지 및 기밀성을 보장하기 위해서 XML 전자서명과 암호화 기술이 사용됨. XML 전자서명 및 암호화 표준은 대부분의 ID 응용 표준기술에 적용 가능한 ID 교환 문서의 암호화와 서명 정보 바인딩 규격을 마련하며, ID 교환문서의 서명용 인증서의 유통과 관리 방법 등에 대한 가이드라인을 마련함

2.1.2. 연관기술 분석

- 연관기술 관계도
  - 개인정보보호 및 ID관리 기술은 개인의 ID에 기반을 둔 모든 기술들과 연관될 수 있으나, 직접적 관계로 표현될 수 있는 기술들은 차세대 웹 기술, 웹서비스 기술, 지적재산관리 기술, 바이오 인식 기술 등이 있음



〈그림 2〉 ID관리기술의 연관기술 관계도

• 연관기술 분석표

연관기술	내용	표준화기구/단체		표준화수준		기술개발수준	
		국내	국외	국내	국외	국내	국외
차세대 웹 기술	웹에 저장된 수많은 데이터에 컴퓨터가 처리 가능한 의미를 부여하여 높은 활용성을 제공하고, 현재의 웹보다 더 넓은 범위의 개방성, 이동성, 연결성 등을 제공하고자 하는 기술로, 차세대 웹에 좀 더 높은 신뢰성을 부여하고자 하는 노력으로 다양한 ID관리 기술이 적용되고 있음	TTA	W3C, OASIS	표준기획	표준안 개발/검토	시제품/프로토타입	시제품/프로토타입
웹 서비스 기술	서로 다른 종류의 컴퓨터들 간에 유연하고 확장적인 방법으로 상호작용할 수 있는 서비스 지향 분산 컴퓨팅 기술로서, 서비스 요청응답 주체의 확인, 상호인증, 서비스 제어, 안전한 메시지 전송 등을 위해서 ID관리 기술을 활용함	TTA, ECIF	W3C, OASIS	표준안 개발/검토	표준화 완료	시제품/프로토타입	상용화
지적재산관리 기술	디지털화된 비디오, 오디오, 문서 등의 콘텐츠의 저작권자(개인, 조직, 정부)를 보호하고 안전하게 유통관리하기 위한 기술로서, 유통과정에서 발생할 수 있는 문제들을 해결하기 위해서 ID관리기술을 채택함	TTA, DRM 포럼	IETF, MPEG21, W3C 등	표준안 개발/검토	표준안 개발/검토	시제품/프로토타입	시제품/프로토타입
IC카드 기술	접근 권한, 개인 인증 정보, 개인의 주요 정보 등을 저장하는 매체로서, On/Off-Line의 열쇠 역할을 담당함. ID관리 기술에서 권한 소지 여부를 확인해야 하는 경우에 사용됨. 바이오인식 기술을 연계할 경우 보다 안전한 운영이 가능함	기술표준원/ ECIF	ISO/IEC JTC1 SC17	표준안 개발/검토	표준안 개발/검토	시제품/프로토타입	시제품/프로토타입
바이오인식 기술	사람의 평생불변 · 만인부동의 특성을 갖는 정보를 획득하여 등록 · 저장하고 이후 제시된 정보와 비교하여 본인인지 여부를 판단하는 기술로서, ID관리 기술에서 본인여부를 강하게 확인해야 하는 경우에 사용됨	TTA, KBA	ISO/IEC, ITU-T OASIS	표준안 개발/검토	표준안 개발/검토	상용화	상용화

2.2. 시장 현황 및 전망

2.2.1. 국내 시장 현황 및 전망

- ID관리 솔루션은 그동안 금융기관과 통신업체를 중심으로 도입이 이뤄지기 시작했다. 2004년부터 서서히 시장이 형성되기 시작해서 2005년 약 100억 원 규모의 시장이 형성됨
- 한국IDC는 2005년도 접근제어를 포함한 전체 계정관리 시장이 246억 원으로 추정하고, 2006년부터 2010년까지 연평균 성장률은 12%로 급성장 할 것으로 전망

〈표 1〉 ID관리 및 접근제어 국내시장규모, IDC, 2006

구분	2005년	2006년	2007년	2008년	2009년	06-10성장률
ID관리 및 접근제어	23,790	24,606	29,527	35,432	42,519	12%

- 국내에서 ID관리 솔루션을 도입한 금융기관은 대우증권, 교보증권, 기업은행 등이 있으며, SK텔레콤, 데이콤 등 통신 사업자와 국민건강관리보험공단, 환경관리공단 등 공공기관도 계정관리 솔루션을 도입했다. 대한항공, 다음커뮤니케이션 등 일반 기업에서도 도입이 활발하게 이루어짐
- 전자정부에서는 행정자치부에서 전자정부 시스템에 통합ID관리 시스템 도입을 추진 중이며, 대전시청의 경우 구축이 완료됨. 정보통신부는 그동안 웹 사이트에서 신원확인 수단으로 사용되었던 주민등록 번호를 대체하는 수단으로 5가지 기술 i-PIN이라고 명명하고 시범서비스를 수행 중
- 전자주민증 및 전자여권, 전자운전면허증 등이 현재 18억 원에서 400억 원 수준의 시범사업이 진행 중. 카드 1장당 약 1만 원정도의 단가가 예상되며, 단말기 등 인프라 설치도 필요하여, 4,000만장의 전자주민증, 2,500만장의 전자운전면허증, 2,400만장의 전자여권 등의 본 사업을 위해서는 각 사업별로 약 2,500억 원에서 수 조원의 비용 투입이 예상됨
- 최근 들어 규제 준수 등을 위해 금융권과 대기업을 중심으로 일부 기업들이 올해 도입을 진행하거나 검토를 진행 중. 산업별로는 금융권에서 대형 금융기관이 계정관리 솔루션을 도입 중이거나 검토 중
- 서서히 계정관리 시장이 확대되고 있는 추세여서 관련업체들도 경쟁이 치열한 상황임. 현재는 대부분 외국계 솔루션 업체들을 중심으로 시장 경쟁이 이뤄지고 있음. 우선 e트러스트 제품군을 중심으로 통합 보안 전략을 펼치고 있는 한국CA는 최근 딜로이트 안진회계법인과 계정관리 준비 평가(IMRA, Identity Management Readiness Assessment) 서비스를 제공하고 있음
- IMRA 서비스는 기업들이 자사가 보유하고 있는 기존의 IT 인프라나 비즈니스 프로세스를 바탕으로 내부 통제적인 측면에서 효과적인 계정 관리 로드맵을 수립하고 구체적인 ROI를 미리 도출할 수 있다는 특징이 있음. CA는 엑스트라넷 액세스 관리 솔루션 업체인 네티그리티를 인수하고 ID관리 솔루션 'CA 아이덴티티 매니저' 를 출시함
- 한국HP는 최근 본사에서 통합ID관리 솔루션 분야의 선두 업체인 트러스트제닉스를 인수한 후 통합ID관리 솔루션 라인업을 강화하고 있음. 그 첫걸음으로 얼마 전 트러스트 제닉스사의 ID를 하나로 통합하는 서버 솔루션인 '아이덴티티 브릿지 2.5 버전' 을 출시함

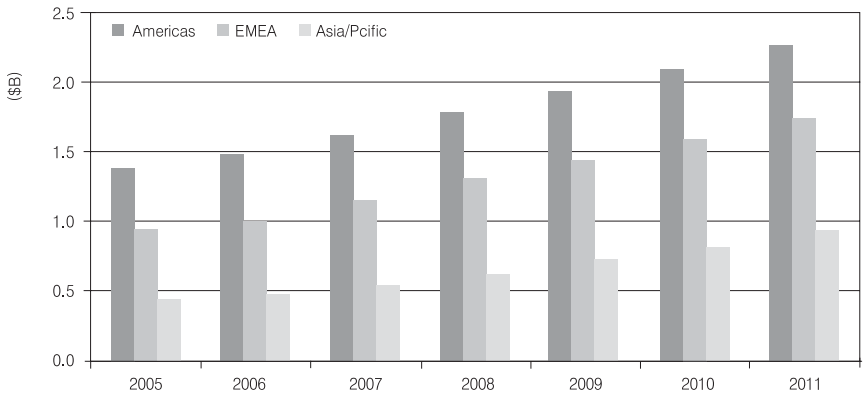
- 한국HP는 트러스트제닉스의 솔루션을 HP의 IT 자원관리 솔루션인 '오픈뷰' 포트폴리오에 통합하는 등 각 제품의 ID 연계 기능을 계속 강화해 나갈 계획임
- 한국IBM은 중소기업에게 적합한 계정관리 소프트웨어 '티볼리 아이덴티티 매니저 익스프레스'로 ID관리 시장에 뛰어 듬. 한국IBM은 내부자 침입 방지 및 컴플라이언스 자동화를 지원하는 이 솔루션을 기존의 시스템 관리 소프트웨어나 보안 제품과 연계해 관련 시장을 공략할 계획
- 한국BMC는 접근 및 컴플라이언스 관리 등을 지원하는 '통합 계정관리 스위트'를 출시하고 본격적인 마케팅 활동을 벌이고 있음. 한국오라클도 최근 본사에서 인수한 계정관리 업체 오블릭스의 관련 솔루션을 국내에 출시하고 활동을 진행 중
- 순수 국내 업체로는 소프트포럼(주)은 ID관리 솔루션으로 SafeIdentity, 이니텍은 INISAFE Nexess, 드림 시큐리티는 Magic SSO & EAM v3.0 제품을 출시하여 기업의 분산된 자원과 사용자를 통합하고 일관된 체계를 구축하기 EAM(Extranet Access Management) 시장을 공략하고 있음

2.2.2. 국외 시장 현황 및 전망

- IDC는 ID관리 및 접근 권한 관리의 세계 시장 규모를 2006년 현재 30억 달러로 산정하고 있고, 2009년에 49억 달러에 이를 것으로 전망

〈표 2〉 ID관리 및 접근제어 세계시장규모, IDC, 2007 (단위, 백만달러)

구분	2005년	2006년	2007년	2008년	2009년	06-10성장률
ID관리 및 접근제어	3,369	3,769	4,151	4,547	4,974	10.7%



〈그림 3〉 지역별 ID관리 및 접근제어 시장규모, IDC, 2007

- ID관리 시장은 ID관리 종합지원 솔루션과 Provisioning, 인증, 연계형 ID 솔루션으로 구분되며 최근 사용자중심 ID 관리 솔루션이 새로이 제공되고 있음
- ID관리 종합지원 솔루션은 조직 내의 인증, 인가, 계정관리, 감사를 모두 수행하는 솔루션으로서 실시간으로 리소스 접근을 제어하기 위한 인증, 인가와 이를 위해 사전에 설정되고 관리되는 계정정보, 이러한 과정들이 사전에 설정된 정책에 위배되는지 감사하는 감사기능을 포함. ID관리 종합 지원 솔루션 벤더로는 CA, IBM, Microsoft, Novell, Oracle, Siemens, Sun microsystem 등이 있음
- Provisioning은 계정관리에 초점을 맞춘 것으로 조직 내에 신규 등록되는 사용자의 인입과 변동되는 계정 정보 등의 관리를 수행함. Provisioning 솔루션 벤더로는 Beta System, BMC, Courion, MaXware, Thor 등이 있음
- 인증은 PKI, 생체, OTP 등 다양한 기술로 인증 강도를 높이고 사용자 편의성을 제공하는 솔루션에 초점이 맞추어 있고 해당 벤더로는 Entrust, Netegrity(CA에 합병), Oblix, RSA Security(EMC의 합병)가 있음
- 연계형 ID관리는 조직 간에 연계된 서비스를 제공하기 위해 ID를 서로 연계하고, 이를 통해 인증, 접근제어 관리 등을 수행하는 솔루션임. 관련 벤더로는 HP, Ping Identity, M-Tech, Trustgenix 등이 있음
- IBM은 2006년, 기존의 Tivoli Federated Identity Manager, Tivoli Directory Integrator, Tivoli Access Manager를 갱신하고 소규모 조직을 위한 ID관리 full suite인 Tivoli Identity Manager Express와 역시 소규모 조직의 federation을 위한 Tivoli Federated Identity Manager Business Gateway를 출시함
- CA는 2007년 SiteMinder, Identity Manager등 기존 제품을 업데이트하였고, XACML(eXtensible Access Control Markup Language), SAML, SPML(Service Provisioning Markup Language)을 지원하는 IAM 툴킷인 Embeded Entitlements Manager를 업데이트 발표함
- 스토리지 부분의 업계선두인 EMC는 RSA Security를 합병함. IDC는 EMC의 스토리지 솔루션에 보안기능을 추가하는 방식이, ID도 결국 스토리지에 저장되는 데이터라는 측면에서 커다란 시너지를 가져올 것이라고 보고 있음
- Verisign은 서비스제공에 집중하고 있으며, "Verisign Identity Protection fraud detection and authentication" 서비스는 클라이언트 로그인과 트랜잭션 정보 보안을 제공함
- Oracle은 Oracle Access Manager, Oracle Identity Manager, Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity and Access Management Suite등 full suite를 제공함. Oracle은 독립적인 IAM 벤더로 관련시장에 진입했으며 업계 5위의 수준에 이르름
- Microsoft는 독점적인 중앙 관리에서 벗어나 여러 ID 제공자의 다양한 ID 기술들을 상호운용하는 ID 메타시스템 개념을 제안하고, 이 개념을 구현하여 윈도우 Vista에 CardSpace로 구현함
- Neustar는 인터넷 상에서 유일한 식별자를 제공하고 데이터를 공유할 수 있는 OASIS의 XRI/XDI 표준을 주도하며 이 표준의 개념을 구현하는 i-names 서비스를 전세계로 발표하였으며, SXIP사 등이 참여한 OpenID 표준은 2006년 말 1,500만 명의 사용자를 가질 정도로 급속히 확장하고 있음
- Sun을 중심으로 세계 150여 개의 업체가 연계한 Liberty Alliance Project는 최근의 표준을 OASIS의 SAML 2.0과 연계하였으며, 이를 기반으로 사용자의 개인정보를 관리하고 공유하는 People 서비스를 공개하여 ID 정보의 매쉬업

이 가능하게 함

- ID관리 기술 및 솔루션의 최신 동향은 시스템 관리 솔루션과 ID관리의 통합, 일반적 감사관리 솔루션에 ID관리 기능추가, 금융권 인증수단 강화 정책, ID관리시장의 세분화, ID 데이터 서비스의 도입, 사용자 중심 ID관리와 ID 메타시스템의 등장을 들 수 있음
- 시스템 관리 솔루션과 ID관리의 통합은 BMC의 Patrol, IBM의 Tivoli, HP의 Openview 등 유명한 네트워크 및 시스템 관리 솔루션에 ID관리 기능이 추가되고 있는 상황을 의미함
- CA, HP, IBM, Novell 등의 감사관리 솔루션이 ID관리 솔루션과 통합되어 제공되고 있음
- 금융권 인증수단 강화정책은 미국의 금융권 규제를 대표하는 US FFIEC(Federal Financial Institutions Examination Council)에서 인터넷 뱅킹에 패스워드를 유효하지 않은 인증수단으로 규정하면서 이를 대체하기 위한 시장이 확대될 전망
- ID관리 솔루션 시장도 적용 조직의 분야에 따라 다양화 되고 있음. 중소기업, 헬스케어, 전자정부, 금융, 교육 분야로 세분화되고 있음. 특이점은 그동안 금융 분야의 솔루션이 상대적으로 부족했으나, 최근에 확대되는 추세에 있음
- ID 데이터 시장이 활성화되고 있으며, 조직이 보유한 ID정보를 외부에 서비스 하는 것이 새로운 형태의 서비스로 관심을 모으고 있음
- 한편 사용자 중심의 ID관리 기술 및 제품이 많은 관심을 모으고 있으며, 인터넷 규모의 ID관리를 수행하기 위해서는 기존의 조직중심의 ID관리나 연계기반 ID관리로는 관리상의 문제로 인한 확장성 제약이 있는 만큼, 사용자에게 제어권을 넘기고 이를 통해 ID관리를 수행하는 ID관리 기술이 활발히 개발되고 관련 솔루션들이 시장에 선보이는 상황임
- 미국 출입시 전자여권을 사용하지 않는 경우, 비자를 발급받아야 함에 따라, 현재 비자 면제국인 선진국들이 서둘러 전자여권 발행을 추진하고 있음. 수년 내에 10억장 이상의 전자여권과 전자운전면허증이 국제적으로 발행될 것으로 예상되어, IC카드용 칩 제조사 및 솔루션 개발사, 단말기 제조사들의 경쟁이 치열해지고 있음. 전자여권의 경우, ICAO에서 상호호환성 시험을 추진하고 있으나 선진국의 일부 기관들의 기능 검증을 끝낸 2006년 이후 추가적인 상호호환성 시험을 추진하지 않아 후발 국가의 기관들은 시험에 어려움을 겪고 있음

2.3. 기술개발 현황 및 전망

2.3.1. 국내 기술개발 현황 및 전망

• 정부정책

- 정보통신부가 추진하고 있는 i-PIN은 대면 확인이 불가능한 인터넷 상에서 주민등록번호를 대신하여, 본인임을 확인받을 수 있는 사이버 신원확인 정보이며, i-PIN은 13자리 숫자나 영문자로 구성되며, 주민번호와 달리 생년월일, 출생지, 성별 등의 개인정보를 포함하지 않음. i-PIN 종류는 5가지로 가상주민번호(한국신용평가정보), 범용공인인증서(한국정보인증), 개인인증키(한국신용정보), 그린버튼 서비스(한국전자인증, 이니텍), 개인아이디인증(서울신용평가정보)이 서비스 중이며, 신원을 확인하는 방법으로 대면 확인, 공인인증서, 신용카드정보, 휴대폰 SMS 등이 가능함
  - i-PIN 제도는 2005년 10월부터 시범적으로 도입된 이후로 2007년 8월 현재 31개 사이트가 도입하여 운영 중이며, 이용이 점차 확산될 것으로 예측됨. MSN(Microsoft Network) 코리아는 최근 네티즌 의견 달기 과정에서의 본인확인 방법으로 i-PIN 을 채택했으며, 국내 대형 포털인 Daum과 Naver 역시 2007년 9월까지 i-PIN 서비스의 도입을 준비하는 과정에 있음
  - 정보통신부측은 주요 포털업체와 공동으로 주민번호 노출 위험성과 i-PIN 이용에 대한 캠페인을 실시할 예정으로, 인터넷 사업자를 대상으로 설명회를 개최하고 i-PIN 적용 사례집과 매뉴얼 등을 배포함으로써 i-PIN 도입을 확산한다는 입장임. 또한, 정보통신부측은 i-PIN 도입 업체에게는 'ePrivacy 마크' 인증 심사 시, 가산점을 부여하는 방식의 회유책을 병행함으로써, i-PIN 보급 확산을 위한 노력을 지속적으로 추진하고 있음
- 정보통신부는 개정 정보통신망 이용촉진 및 정보보호 등에 관한 법률(정보통신망법)'과 시행령 및 시행규칙을 2007년 7월 27일부터 동시에 시행함. Naver와 Daum 뿐만 아니라 하루 평균 이용자가 30만 명이 넘는 포털 사이트 및 20만 명 이상 인터넷언론사 사이트 등 33곳에도 제한적 본인확인제를 확대 · 도입함. 개정 정보통신망법의 주요 내용으로 제한적 본인확인제, 정보접근 임시차단조치제도, 명예훼손분쟁조정부 신설, 개인정보 보호 강화, 친북게시물 등 불법정보에 대한 장관명령권 대상 확대가 있음. 그 중에서 제한적 본인확인제는 1,150개 공공기관 등과 35개 인터넷서비스사업자(포털, 인터넷언론, UCC사업자)가 운영하는 게시판에 이용자가 정보를 게시하려면 먼저 본인여부를 확인 받아야 함. 해당 이용자가 본인확인을 받고 난 후에는 ID, 별명 등을 자유롭게 사용할 수 있도록 함. 또한 개인정보의 수집 · 이용 · 제공에 대한 고지 및 동의 제도를 개선, 사업자는 개인정보 수집시 수집 및 이용 목적, 수집항목, 보유 및 이용기간, 제3자 제공에 관한 사항을 이용자에게 명확히 알리고 동의를 받아야 함. 또 개인정보취급에 대한 제반 방침을 이용자가 언제든지 확인할 수 있도록 취급방침을 공개해야 함. 사업자가 개인정보를 취급할 수 있도록 업무를 위탁하는 경우에는 이용자로부터 동의를 얻어야 하며, 개인정보 파기 사유에 사업폐지의 경우'가 추가됨
- 전자정부 등 주요 정보화 사업들이 본격 추진되고 있으나, 정보시스템에 대한 공통된 기술적 기본 방향 및 기준이 부재함에 따라 정보화 사업의 효과 저하, 상호호환성 저하, 일정 수준의 품질 확보 미흡, 인터페이스 표준화 부재로

인한 연계의 복잡화, 표준 사용의 효과 반감이 우려됨. 따라서 정부혁신지방분권위원회와 정보통신부, 한국전산원은 정보화시스템 구축시 준수해야 할 최소한의 기술 기준을 명시한 '정보시스템 구축, 운영 기술 가이드라인'을 작성하여 정보시스템의 상호호환성, 사용자 편의성, 보안성 등 최소한의 품질을 확보하기 위한 지침을 마련함

◦ 기술 가이드라인은 여러 파트로 구성되어 있으며, 보안 파트에서는 디지털 ID의 안전한 관리를 위해, 보안이 중요한 서비스 및 주요 데이터 접근에 대한 사용자 인증은 PKI 기반의 행정전자서명 또는 공인전자서명을 사용하도록 명시하고 있음. 또한 웹 서비스를 통한 시스템 연계시, 사용자 인증 정보의 연계에는 SAML 1.1을 사용하여 사용자 정보를 기술할 것을 권고하였으며, 웹 서비스 및 XML 보안을 위해 WS-Security와 SAML의 사용을 권고함

– 행정자치부는 공공기관에서의 개인정보보호를 위한 ID 관리 체계 구축을 핵심으로 한 통합ID관리 서비스를 추진하고 있음. 통합ID관리 서비스는 정부부처 및 지방자치단체, 공공기관 등의 사이트에 다양하게 산재되어 있는 회원들의 개인정보를 안전하게 보호, 관리하는 서비스로서, 행자부는 2007년에 중앙행정기관 및 지방자치단체 300여 기관에 서비스를 도입하는 것을 시작으로 2008년에는 각급 교육기관 및 기타 행정기관 1만 3000여 곳, 2009년에는 서비스 이용을 희망하는 공공기관으로 서비스를 확대한다는 3단계 추진 계획을 마련함

◦ 통합ID관리 서비스는 SAML 2.0과 Liberty Alliance의 ID-WSF 2.0 표준을 준용함. ID 센터는 ID 제공자 역할을 수행하며 공공기관은 서비스 제공자 역할을 담당하며, 사용자가 공공기관에 가입을 시도할 때마다 ID 센터에 로그인하여 발급받은 식별정보로 본인 확인 절차를 통과하게 됨. 이 시스템은 공공기관에 통합계정을 신청한 이용자의 정보는 ID 센터에 전달돼 부여된 다른 고유의 식별번호로 인증 · 저장 · 관리되는 방식으로 이뤄져 있어, 이 번호가 유출되더라도 다른 공공기관에서 사용할 수 없으며 주민번호가 도용됐어도 공공기관 사이트 회원가입과 이용할 수 없어 개인정보 유출을 방지할 수 있음

◦ 행정자치부의 통합ID관리 서비스와 관련하여, 대전광역시에서 지역정보화지원사업비 5억4,000만 원을 지원받아 2006년 6월부터 12월까지 시범사업으로 추진함. 공공기관 통합ID관리 시스템(http://idsp.go.kr)은 대전시청 홈페이지를 비롯하여 16개 사이트와 연동되며 서비스가 보급되면 시민들은 공공기관 사이트들에서 통합ID관리 서비스를 통해 주민등록번호등의 본인 여부를 확인하는 대체 수단으로 사용할 수 있게 됨

◦ 행정자치부는 현재 전자주민증인 주민등록 발전모델에 대한 시험발급 사업을 추진 중임

– 행정자치부는 '공공기관의 개인정보보호에 관한 법률'의 주요내용을 2007년 5월 17일 개정 · 공포함. 이번 개정안에는 공공기관의 과도한 개인정보 수집을 방지하기 위해 현행 개인정보파일의 '사전통보제'를 '사전협의제'로 개정, 개인정보파일을 보유하거나 변경할 때 목적과 범위 등을 사전에 개인정보보호심의위원회와 협의토록 함. 또한 공공기관은 개인정보의 보호 · 관리를 위한 책임관을 지정토록 했으며, 개인정보의 수집, 이용 · 제공, 위탁관리, 폐기 등의 경우에는 인터넷에 공시하도록 의무화해 앞으로 보다 안전하고 투명하게 개인정보가 관리될 전망

◦ 인터넷상 본인확인 과정에서 주민번호, 성명 등 개인정보가 변조나 유출, 도용되지 않도록 통합 ID관리 서비스 등 안전성 확보에 대한 의무도 부과함

◦ 공공기관이 보유한 개인정보에 대한 국민들의 '자기정보통제권'을 강화하기 위해 정보의 삭제를 청구할 수 있는 '삭제청구권'을 신설했으며 본인정보의 열람청구 시 그 처리시한을 현행 15일에서 10일로 단축함. 개인정보주체

가 본인의 정보를 침해당했을 경우, 이를 신고해 시정토록 하는 '개인정보침해사실 신고제'와 정보주체의 분명한 인식 아래 개인정보가 수집될 수 있도록 개인정보 수집시 법적근거, 수집목적 등을 인터넷 등에 게재해야 하는 규정도 마련함. 이 법안은 2007년 11월 18일부터 시행됨

• 기술개발

- 국내의 OpenID 시장은 2007년부터 시작되었으며, 현재 NC소프트(http://myid.net), 이니텍(http://idpia.com), 안철수연구소(http://idtail.com), Daum(http://openid.daum.net)이 OpenID 제공자로 동작하고 있음. OpenID 소비자로는 NC 소프트의 스프링노트, 미투데이, 라이브팟이 있다. 최근 대형 포털 및 인터넷 사업자들도 OpenID 적용에 관심을 보이고 있으며, Paran과 Egloos 등은 자사의 URL을 OpenID로 사용할 수 있는 기능을 제공함. OpenID 국내 커뮤니티(http://openid.or.kr)와 포럼은 OpenID 제공자들과 ETRI 등이 참여하며, 스펙 번역과 개발, 동향 관련 정보를 공유하는 상황임
- 이니텍은 OASIS의 XRI 표준을 준용한 i-broker 서비스(http://www.gbtn.biz)를 2006년 7월 12일 시작함. i-broker는 전세계적으로 진행되는 GRS(Global Registry Service) 프로그램을 따른 것으로, 전세계적인 규모로 서비스를 제공하며 타 i-broker와도 동일하게 동작함. XRI 표준을 따르는 ID를 i-name이라고 하며, i-name을 등록한 사용자는 ISSO(단일 로그인), Contact(연락처), Forwarding(메일 필터링) 서비스를 제공받게 됨. i-name을 Id로 SAML 인증 사이트 및 OpenID 인증 사이트에 접속할 수 있도록 SAML을 이용한 인증과 OpenID 인증 방식을 지원함
- 인터넷식별자포럼(http://www.uriforumor.kr)은 인터넷에 존재하는 정보자원과 콘텐츠의 위치 확인 및 검색을 가능하게 하는 인터넷 식별체계를 다루고 있으며, 대표적인 인터넷 식별체계로는 영문, 한글 도메인과 IP 주소, 모바일 인터넷 주소, 전화번호를 이용한 ENUM(E.164 Number Mapping) 등이 존재함. 한국인터넷진흥원(http://www.nida.or.kr)은 국가인터넷주소자원 관리기관으로 전 분야에 걸친 이슈를 담당하고 있으며, 최근 한국인터넷진흥원은 인터넷 관련 국제기구들과의 협력을 통해 최신 정보를 공유하고 동향 파악에 힘을 기울이는 한편, 내부 연구역량 강화에 특히 주안점을 두고 있음. 차세대 인터넷 식별자의 표준화와 관련된 핵심 기술인 '보편적자원식별자(URI, URL과 URN을 포함하는 개념)' 표준화에 적극 나서고 있음
- ETRI는 2004년부터 2006년까지 수행된 'e-Identity 보호용 공통보안 서비스 플랫폼 기술개발' 과제에서 OASIS의 표준인 SAML 2.0과 Liberty Alliance의 표준인 ID-WSF 2.0, ID-SIS(IDentity Services Interface Specification) 2.0을 채택하여 e-IDMS(etri-IDentity Management System)을 개발함. 공동연구기관인 소프트포럼(주)은 해당 기술을 이전받아 행정자치부의 시범사업인 대전시청 통합ID서비스 구축에 활용함. 또한 모바일 환경에서 ID-WSF 2.0의 인터렉션 서비스를 적용하여, 공인인증서 기반의 콜백 URL SMS를 이용한 모바일 인터렉션 서비스 기술을 개발함

◦ 2005년 8월, ETRI는 Liberty Alliance의 주관으로 미국 뉴저지주의 Piscataway의 IEEE-ISTO에서 열린 OASIS SAML 2.0 표준에 대한 제1회 상호호환성 시험을 통과함

◦ 본 기술은 관련 업체에 기술이전 되어 행정자치부의 시범사업인 대전시청 통합ID 서비스 구축과 ITEC 공통서비스 구축 등에 활용됨

- 소프트포럼은 ID관리 솔루션으로 SafeIdentity를 개발하였으며, 멀티도메인 간, 다양한 어플리케이션 간의 통합인증(SSO) 제공, 역할기반접근제어(RBAC, Role-based Access Control) 시스템 제공, 정책기반의 관리 기능 제공, 고도의 사용자 개인화를 통해 자동 사용자 요청 및 승인 프로세스 지원, 감사 보고 기능이 가능함
- 이니텍은 INISAFE Nexess를 통해 기업의 분산된 자원과 사용자를 통합하고 일관된 체계를 구축하는 EAM 솔루션을 제공하며, ID/PW, PKI, 지문인식, OTP, MOTP(Mobile One-Time Password), Smart Card 등 다양한 인증 방식뿐만 아니라 Multi-Domain에서의 안전한 SSO가 가능하고, 또한 RBAC 기반의 권한 관리, 중앙집중적 통합 관리와 관리자 위임 기능을 통한 분산적 관리 기능을 제공함
- 티맥스소프트의 SysKeeper EAM은 역할기반 접근제어를 수행하는 Policy 서버를 중심으로 Proxy 서버에서 인증 및 접근제어를 처리하는 모델과, WAS/WEB Agent에서 인증 및 접근제어를 처리하는 모델로 구성되어 있고, 또한 디렉토리 정보가 통합되지 않는 ERP,그룹웨어, 메인프레임 등의 시스템은 커스템 인터페이스를 통하여 기존 시스템과 통합 관리될 수 있으며, 자사의 WAS 솔루션과 결합하여 EAM 기능을 처리함
- 펜타시큐리티시스템의 ISign은 SSO 기능을 기본적으로 제공하면서 통합 권한 관리 기능을 제공하는 EAM 솔루션이며, SSO 기능은 전자정부 및 공인인증기관의 PKI 인증서를 지원하며, 속성 인증서(Attribute Certificate)를 이용한 사용자 권한 제어와 RBAC 기반의 권한 설정 정책을 제공함. 또한 ISign의 Roaming 기능은 사용자에게 키 로밍을 통한 사용자 인증과 접근 제어를 다양한 환경에서 보장하여 사용자의 이동성을 증가시켜줌
- 드림 시큐리티는 다양한 인증방식(ID/PW, 인증서, 생체인식, cd-key)을 지원하며 인증 단계에 따른 권한을 선택적으로 부여하는 SSO 솔루션인 Majgic SSO & EAM v3.0 제품을 개발함. 사용자인증 및 ACL 발급을 담당하는 인증서버(Policy Server)와 사용자 PC에 설치되고 사용자인증 후 세션을 관리하는 클라이언트 에이전트(Client Agent), 사용자 및 권한관리가 필요한 어플리케이션을 등록하고 권한을 관리하는 인터페이스인 관리자 어드민(Policy Server Admin)으로 구성되어 있음
- 알툴즈(ALTools) 사의 알패스는 회원제로 운영되는 많은 웹사이트의 아이디와 비밀번호를 관리할 수 있는 프로그램으로, 2007년 7월 19일 버전 3.02가 배포됨. 알패스는 클라이언트와 서버로 구성되어 있으며, 클라이언트는 사전에 ID/PW 데이터를 서버에 등록하고 암호화된 랜덤키를 저장하고 있다가 특정 사이트에 로그인할 때 해당 랜덤키로 사이트에 로그인하는 방식을 사용함. 로그인 정보 자동 채움 기능을 제공하며 부가적으로 USB 연동, 온라인에 데이터를 저장함으로써 데이터 손실 회피, 개인정보 노출 방지 기능이 가능함
- SecuTronix의 이지패스는 웹에서의 로그인뿐만 아니라 각종 메신저 및 응용 프로그램의 로그인까지 지원하는 제품으로, 2007년 8월 현재 2.0.4 버전이 릴리즈됨. MSN, 네이트온과 같은 메신저 로그인과, Melon, JukeOn 등의 응용프로그램 또한 현재 지원 중임. 추가적으로 USB에 탑재하여 사용할 수 있으며, 한 사이트에 여러 계정을 보유한 경우 또한 지원함. 이지패스 솔루션은 ID/PW 방식의 로그인을 기반으로 하며, 지문인식기가 제공된 경우 지문인증으로 로그인이 가능함

- ETRI는 Microsoft, KISA는 '전자ID지갑' 시스템 개발에 착수. 전자ID지갑은 사용자 본인이 개인정보와 인증정보(ID/PW, 인증서 등)를 안전하게 관리하고 있다가, 언제 어디서나 자신을 인증하고 개인정보를 자신의 통제 하에 선택하여 이용할 수 있는 시스템임. 2007년부터 2009년까지 3년간 수행되는 '자기통제 강화형 전자ID지갑 시스템 개발' 과제는 i-PIN, OpenID, CardSpace 등의 관련 표준들과 호환되며, 오픈소스 환경뿐만 아니라 모바일 환경에서도 동작하도록 개발될 예정임
- P3P의 에이전트 S/W는 '05년 KT가 프라이버시 보호 선도 기업 이미지 제고를 위한 고객 서비스의 일환으로 향후 부가기능(전자지갑, 일정관리, 정보관리 등)을 패키지로 해서 메가패스 고객 및 신규 고객에게 배포하고 가능하다면 모든 이용자를 대상으로 보급을 계획하고 자발적으로 PAgent를 개발함
  - PAgent는 사이트를 정책 충돌 여부 등을 판단하여 신뢰도를 5등급으로 나누어 결과 값을 5가지 색으로 표시하고 경고음, 팝업창 등을 통해 결과를 구현하고 각각의 정책에 대한 수준을 설정하고 해당 정보에 대한 접근수준, 수집 · 이용 목적 항목을 설정할 수 있으며, 방문사이트의 이력관리, 신뢰사이트 등록 등을 지원함
  - P3P의 정책생성 S/W는 '05년 개인정보보호를 위한 기술적대책의 일환으로 학계 · 이용업계 · 정부 등으로 구성된 P3P 연구 작업반 운영을 통해 KISA가 서버용 생성기를 개발함
- ETRI에서 2005년 XACML2.0 API를 개발하였으며, 포스테이터의 BizSafe가 XACML1.0을 지원하며 이들 XML 기반 접근제어기술은 데이터의 접근 제어를 수행함
- ETRI는 또한 1999년부터 2002년까지 수행된 '차세대 IC카드 개발 사업' 및 2003년부터 2004년까지 수행된 'IMT-2000용 USIM 개발 사업'을 수행하면서, IC카드 관련 핵심 기술을 보유하고 있으며, 2001년부터 현재까지 교통카드 및 지급결제 관련 표준화를 추진하며, IC카드의 응용 기술에 대한 노하우를 보유하고 있음
- 국내 암호기술은 SEED, ARIA, CRYPTON, HIGHT 등의 대칭키 암호알고리즘과 전자서명 알고리즘 KCDSA, 그리고 해쉬 알고리즘 HAS-160과 FORK-256등 다양한 원천기술과 NIST의 CMVP와 유사한 암호모듈검증제도 등과 같은 다양한 안전성 평가 기술들을 보유하고 있음
- 암호와 관련된 다양한 연구가 대학과 연구소 등에서 활발히 이루어지고 있고, 현재 정보보호 선진국과의 기술 격차가 1~2년 정도 뒤져있다고 평가되고 있음
- XML 문서의 안전한 유통을 위한 XML 전자서명기술, XML 암호화기술, SAML, XACML 등의 기술이 ETRI에서 개발하여 보유하고 있음
- 국내 전자서명 인증관리 체계에서는 인증서 규격으로 X.509 v3 인증서를 사용하여 PKI에서 사용하는 공개키, 개인키와 같은 비대칭키를 관리하고 있음

〈표 3〉 국내 ID관리 및 접근제어 솔루션 개발 현황

구분	기관	내용
EAM	드림 시큐리티	- MagicSSO, MagicAccess - PKI 기반의 인증서 이용 SSO 지원 - 서버별 사용자 접근 권한 부여 및 확인
	소프트포럼	- SafeSignOn - PKI 기반의 인증서 이용 SSO 지원 - 통합적 권한 관리 - SAP, IBM 등 솔루션업체와의 제휴 및 연동 - 웹환경과 C/S환경 지원
Federated ID	소프트포럼	- SafeIdentity - 멀티 도메인간, 다양한 어플리케이션 간의 SSO 제공 - 정책 기반 관리 - Self-Profile 관리 모듈을 통해 사용자 프로파일 수정과 자동 사용자 요청, 승인 프로세스 지원 - 로그 데이터를 기반으로 한 보안 감사 및 통계 리포팅 작업 지원, 감사 데이터 백업 및 삭제 기능
User-Centric ID	이니텍	- I-names, OpenId - 2006년 6월부터 gbtn,biz를 통해 i-names 서버를 제공함 - 2007년 상반기에 OpenID 서비스를 제공할 예정임
	OpenMaru	- myid,net - NCSoft 계열사 - OpenID 서버를 제공하는 국내 최초의 서비스 - URL을 식별자로 하여 OpenID를 지원하는 사이트에서는 OpenID를 사용하여 SSO를 제공함
	IDtail	- Ahn, Lab 계열사 - OpenID 서버를 제공 - URL을 식별자로 하여 OpenID를 지원하는 사이트에서는 OpenID를 사용하여 SSO를 제공함

• 전망

- 2007년도 IDC 보고서에 따르면, 국내의 대표적인 IAM 관련 기업인 소프트포럼, 펜타시큐리티, 시큐어소프트, 티맥스소프트, 어울림 정보통신은 전세계적으로 미미한 점유율을 보임. 하지만 2005년 690만 달러와 2006년 700만 달러의 매출을 기록하는 등, 최근에는 전체 평균 성장률인 8.1%를 상회하는 연간 20% 내외의 급격한 성장을 보임

2.3.2. 국외 기술개발 현황 및 전망

• 정부정책

- 미국은 지난 2003년 ID/PW, PKI, 바이오정보 등을 통한 사용자 인증 프레임워크를 제공하기 위하여 크리덴셜의 안정성 기준과 발급기관의 신뢰성 평가 등을 포함한 e-Authentication 정책을 수립하여 추진 중. NIST(National Institute of Standards and Technology)는 크리덴셜 기술표준 개발, 크리덴셜 발급기관의 신뢰성 평가, 크리덴셜 발급 및 검증 솔루션에 대한 상호호환성 테스트를 수행. e-Authentication initiative는 온라인 환경에서의 새로운 인증관련 비즈니스 모델을 개발하는 '전자인증 파트너십(Electronic Authentication Partnership)'을 추진하고 있으며, 2007년 6월 미 연방정부의 전자인증 프레임워크를 지원하는 Relying Party의 수는 2007년 2분기에 46개에서

3분기에는 51개로 늘어나며, 2007년 4분기에는 80여 개에 달할 것으로 예측

◦ OASIS와 미 조달국(GSA)은 2005년 2월 미국 샌프란시스코에서 개최된 '2005 RSA Conference'에서 에 대해 SAML v2.0 상호운용성 데모를 실시. 데모에는 인증기술의 상호운용성 등을 검증하는 OASIS Federated Identity InterOp Lab, 전자정부/전자인증을 담당하는 GSA의 E-Gov E-Authentication Initiative와 함께 실시되었으며, CA, HP, Entrust, RSA Security, Sun Microsystems 등 13개 사가 참가

◦ 2007년 5월에 발간된 e-Authentication의 기술 아키텍처 가이드라인 v2.0에 따르면 연계된 ID공유 스킴으로는 OASIS의 SAML 표준을 지원한다고 명시되어 있으며 자세한 적용 방안을 설명하고 있음. 이 문서에서는 e-Authentication을 위한 제품들은 2007년 내에 SAML 2.0 SSO 프로파일을 적용하도록 명시되어 있음. 또한 e-Authentication 상호호환성 연구실에서 SAML 표준을 준용한 제품들의 상호호환성을 시험하고 있으며, 이미 CA, HP, IBM, Novell, Oracle, RSA, Sun 등의 기업 제품이 테스트를 통과함

◦ 2001년 9.11 테러 이후 미국은 미국 입국신청자를 대상으로 생체정보 탑재 여권 및 비자 소지를 요구하였으며, 테러방지를 위해 2002년 5월 '국경보안 강화 및 비자 개혁법' (Enhanced Border Security and Visa Reform Act)을 제정함. 이후 UN ICAO(국제민간항공기구)에서 ISO/IEC JTC1/SC17/WG3에 여권 및 비자(사증)에 관한 표준 제정 의뢰하는 등 국제 전자여권 표준을 주도하였고 2006년 규격 개정을 완료하여, 2007년 10월 ISO에서 해당 규격을 국제표준으로 제정할 예정

- 유럽연합(EU)은 'i2010 전자정부 실행계획'에 따라 2010년까지 상호인정 및 연동 가능한 디지털 ID관리 프레임워크 구축을 목표로, 2007년에는 상호호환 가능한 디지털ID관리 기술의 공통사항 합의, 2008년에는 대규모 시험 프로젝트의 운용 및 관찰을 거쳐 2010년까지 범 유럽 차원에서 운용할 수 있는 디지털 ID관리 시스템 구축을 추진 중이다. 대표적인 관련 기술연구 프로젝트로는 FIDIS(Future of Identity in the Information Society), GUIDE, MordinisIDM, PRIME(Privacy and Identity Management for Europe), adapID(advanced applications for electronic Identity cards in Flanders) 등이 있음

◦ EU는 2006년부터 여권 없이 국경 통과가 가능하며, 운전면허증 기능을 통합한 EUID라는 유럽 공통 ID카드 개발을 추진하고 있음

- 오스트레일리아는 정부 부서의 관할 하에 빅토리아 주 정부의 프로젝트인 VBMK(Victorian Business Master Key) 프로젝트를 통해 정부의 중요 정보를 비즈니스에 쉽게 사용할 수 있도록 함. 연계된 SSO 기능을 제공하여 사업자들이 한 번의 로그인으로 여러 정부 부처가 제공하는 정보를 사용할 수 있도록 함. 2006년 2월부터 SAML 2.0 기술을 적용하여 SSO 기능을 제공 중. VBMK 프로젝트는 3년 동안 6백만 호주 달러(약 48억원)로 운영되고 있으며, 현재 VBMK는 매년 65000 명의 비즈니스 가입자를 신규로 받고 있음

- 일본은 사용자의 개인정보 보호를 위하여 신뢰기관을 통한 사용자 인증기반을 마련하고자 차세대 전자인증 프로젝트를 진행 중. 크리덴셜 서비스제공자, 서비스 제공자 등이 적절한 인증수단을 선택할 수 있도록 가이드라인을 제시하고 SAML과 같은 표준 명세에 기반하여 상호호환성이 보장된 인증서비스가 제공될 수 있도록 기반을 마련함

◦ 세부 내용으로는 차세대 인증 적용 시 관련되는 참여자를 식별하고 크리덴셜 발급과 관련하여 필요한 시나리오

개발을 위해 전자인증 업무 모델 체계를 수립. 또한 인증프레임워크, 보증레벨의 결정을 위한 절차, 운영 및 기술기준으로 구성된 인증가이드라인을 개발하고, 사용자와 인증서비스 제공자간 계약 시 참조될 수 있는 합의서 등의 템플릿을 제공할 예정

◦ 일본에서는 2006년 4월부터 전국민 대상으로 전자주민증을 보급하고 있으며, 미국입국을 위한 전자여권 개발에서 앞장서 전자여권을 현재 시험발급하고 있음

- 중국의 교육부는 세계에서 가장 큰 그리드 컴퓨팅 프로젝트인 ChinaGrid를 구축하여, 중국 100개 대학의 20만명의 학생을 연결하였다. 저장소간에 사용자 정보 교환은 SAML2.0 스펙을 따름
- 웹사이트 이용자들의 효과적인 개인정보보호방침 확인을 위해 요약 방침, 다단계 고지 방법 등의 채택을 권고하는 국제적 움직임이 있으며, APEC, OECD 등 주요 국제기구 연구반에서 방침에 대한 고지를 개인정보보호 분야 주요 현안으로 다루고 있고 기업뿐만 아니라 호주, 뉴질랜드, 온타리오와 같은 다양한 정부들이 다단계 고지를 적극적으로 활용하고 채택함

◦ 캐나다의 경우 BC와 온타리오에서 Healthcare 분야에서 다단계 고지를 도입

◦ 호주의 경우 프라이버시법에서 간략한 프라이버시 고지를 활용할 것을 장려하고 정부 분야에서는 세계에서 처음으로 '05.7월부터 다단계 고지를 웹사이트에 게시함

◦ 미국의 경우 US Postal service가 웹사이트에 다단계 고지를 도입함

• 기술개발

- 2007년 7월, OpenID는 약 4,500여 개의 사이트에서 사용되고 있으며 발급된 id의 개수는 1억 2천여 개에 달함. 현재 2.0 버전의 인증 스펙은 11번째 드래프트 버전이 공개되어 있고, 1.0 버전의 속성 교환 스펙은 5번째 드래프트가 공개. 또한 Simple Registration Extension 1.1 스펙과 Provider Authentication Policy Extension 스펙의 드래프트 버전이 공개됨

◦ 미국의 대형 포털인 AOL은 OpenID 제공자가 되어 자사의 고객이 별도의 작업 없이도 OpenID를 사용할 수 있도록 함. Yahoo는 자사의 인증 API인 BBAuth를 이용하여 가입자에게 OpenID를 제공. 대표적인 블로그 업체인 Six Apart는 자사의 LiveJournal과 Vox 사이트에 OpenID를 적용함. 또한 SUN은 자사 직원에게 OpenID를 제공하기로 하고, 자사의 SSO 솔루션인 OpenSSO와 OpenID 라이브러리를 통합하여 서비스를 구축

◦ JanRain, Heraldry 등을 비롯하여 여러 업체와 단체에서 OpenID 라이브러리를 오픈소스로 제공하고 있으며, C#, C++, Java, Perl, Python, Ruby, PHP, ColdFusion 언어를 지원

- i-name은 NETSTAR, Cordance, xdi.org가 인프라를 담당하고 있는 사이트로 OASIS의 XRI 표준을 적용한 서비스를 제공. 전세계적으로 XRI 주소를 해석해주는 역할을 수행하고 있으며, 현재 11개의 서비스 제공자가 가입되어 있음. ooTao의 EZ iBroker, 2idi, LinkSafe, 1id.com, 영국의 =you, CIM3, EnCirca, The Customer's Voice, JanRain, Vibrant, 그리고 한국의 Initech이 제공하는 Green Button이 있음. 이들 서비스 제공자는 GSS(Global Services Specifications)에 따라 서비스를 구축하며, GSS는 법적, 관리상의 정책, GRS의 운영 · 등록 · 주소해석

정책 등을 명시함. 최근 i-name 서비스는 OpenID를 지원하기로 하였으며, 기존의 URL 방식이 아닌 XRI 포맷의 식별자로도 OpenID를 사용할 수 있도록 함. 오픈소스 커뮤니티에서도 XRI 표준을 개발하려는 시도가 이루어지고 있으며, OpenXRI 프로젝트에서 Java 버전의 라이브러리를 2006년 8월에 공개함

- Liberty Alliance는 자사의 ID-FF, ID-WSF, ID-SIS 표준을 작성한 이후, 이들 표준의 내용을 OASIS SAML 표준에 적용시킴. 또한 SAML의 활성화에 많은 노력을 기울였으며, 여러 SIG(Special Interest Group)을 운영하여 기술적, 정책적인 관점과 전자정부, 의료 분야 등의 관점에서 가이드라인과 최우량 사례(Best Practice)를 도출함
  - 최근 Liberty Alliance는 자사의 표준에만 국한되지 않고, ID관리 분야의 타 표준과 연동하여 시너지를 높이는 방안을 고려하고 있음. Concordia 프로젝트로 명명된 이 작업은 Liberty Alliance의 ID-WSF 표준을 비롯하여 CardSpace, OpenID, SAML2.0, WS-Federation 기술들이 상호호환되는 사용 예를 도출하고 요구사항을 정의하는 중. 2007년 7월 28일, Liberty Alliance는 다른 ID관리 표준들과 함께 동작할 수 있는 새로운 ID 프레임워크로 IGF(Identity Governance Framework)를 공개. IGF 프레임워크는 OpenID, WS-*, Bandit, Higgins, CardSpace와 호환될 수 있도록 작성될 예정이며, 작성된 표준은 HP와 Oracle이 개발할 제품에 활용될 예정
  - 또한 Liberty Alliance는 openLiberty.org라는 사이트를 운영하면서, 조직이 보유하고 있는 표준을 오픈소스로 구현할 계획. 가장 먼저 ID-WSF 2.0의 오픈소스 라이브러리를 개발 중
  - 상호호환성 시험에서 Alcatel, CA, Elios, Entr′ouvert, Ericsson, Gemalto, HP, IBM, Nokia, Novell, NTT, Oracle, Ping IDentity, Sun, Symlabs는 ID-FF 1.x 스펙의 상호호환성 시험을 통과. HP, Nokia, Novell, NTT, Sun, Epok, Gemalto, Symlabs는 ID-WSF 1.x 스펙의 상호호환성 시험을 통과. HP, NTT, Symlabs는 ID-WSF 2.0 스펙의 상호호환성 시험을 통과. HP, Intel, NTT, SYmblab는 Liberty Alliance의 Advanced Client 스펙의 상호호환성 시험을 통과
- AOL은 외부의 어플리케이션이 AOL의 온라인 서비스에 쉽게 접근하여 상호동작할 수 있기 위해 Liberty의 ID-WSF 기술을 적용. 이로 인해 2005년 10월, D-LINK는 AOL의 인터넷 브로드캐스팅 서비스인 Radio@AOL를 접근할 수 있게 되었으며, 2,400만 명의 사용자들에 해당 서비스를 제공해 줌
- 일본 NTT Communication은 Liberty Alliance의 Federation 기술을 적용하여 400만 가입자들에게 MasterID라는 SSO서비스를 제공. 또한 2007년 7월 3일, NTT Communication은 NTT 레조난트 주식회사의 gooID와의 제휴를 통해 통합 서비스를 제공하기 시작. 본 제휴는 NTT 소프트웨어 주식회사의 TrustBind/Federation Manager 기반 제품으로 가능하며, 이 제품은 Liberty의 상호호환성 시험을 통과한 것
- 프랑스 텔레콤은 Orange 프로젝트를 통해 Liberty ID-FF 기술로 자사의 5,000만 사용자에게 SSO 서비스를 제공하였으며, 2006년 2월에는 1,000만 사용자에게 소액 지불 서비스인 Wanadoo를 제공
- Google은 자사의 솔루션인 Google App에 SSO 및 인가 기능을 제공하기 위해 SAML 2.0 표준을 지원. Google은 Google Apps를 기업용 버전과 교육용 버전을 배포하였으며, 2006년 10월 미국의 아리조나 주립 대학은 이 제품을 도입하기로 결정하였으며 2007년 말까지 6만 5천명의 학생들에게 서비스를 제공할 예정. 또한 2007년 4월 일본 대학교에서 10만 명의 학생에서 서비스를 제공하기로 함. 일본 대학교는 향후 졸업생과 교직원을 포함하여 50만 명

에게 서비스를 확대할 예정

- AOL은 파트너 사이트와 SSO를 제공하여 사용자에게 편의를 주기 위해 SAML 2.0을 도입. 사용자가 우선 AOL에 로그인 한 뒤에, AOL에서 링크로 연결된 파트너 사이트에만 SSO 기능을 제공
- SAML 2.0 상호호환성 시험에서 CA, Entr′ouvert, Entrust, Ericsson, HP, NTT, NTT Software, Oracle, Ping Identity, Symlabs, IBM, NET, Novell, Reactivity, RSA Security, Sun이 통과
- Shibboleth 프로젝트는 American Chemical Society를 비롯한 20개 기관이 Information Provider로 동작하며, GridShip과 Napster를 비롯한 25개 시스템과 연동. Condor-Shib, Grid-Shib, Project Sentinel Collaboratory와 같이 미국 내에서의 연동 프로젝트뿐만 아니라, SAML을 기반으로 노르웨이의 교육센터에 federated ID관리를 제공하는 FEIDE(Federated Electronic Identity), 덴마크의 고등 교육기관의 리소스 관리를 위한 DK-AAI 프로젝트, 스웨덴의 교육기관을 대상으로 SAML기반의 federated ID 서비스를 제공하는 SWAMID(SWedish ACadeMic IDentity), 스위스의 SWITCH(Swiss Education and Research Network) 인증 인가 인프라(Authentication and Authorization Infrastructure(AAI)), Shibboleth를 테스트한 영국의 SDSS(Shibboleth Development and Support Services)과 실제로 제품화를 시작한 영국의 Access Management Federation for Education and Research 프로젝트, 영국의 JISC Core Middleware Initiative, 오스트레일리아의 고등 교육기관을 위한 연계된 IAM 인프라를 구축하는 MAMS(Meta-Access Management System), 프랑스의 고등 교육 기관을 대상으로 국가적인 federation을 구축하는 목적으로 2006년 10월에 제품화를 시작한 CRU 프로젝트, 핀란드 대학간의 ID Federation을 통한 SSO를 제공하는 Haka 등의 국제적 프로젝트가 있음
  - Shibboleth는 2007년 8월 현재 1.3 버전이 릴리즈되어 있으며, OpenSaml 2.0 이 정식으로 릴리즈된 이후에 Shibboleth 2.0이 진행될 예정. OpenSaml 2.0은 2007년 6월 18일 alpha1, java edition이 릴리즈된 상태이다. 전세계에 걸쳐 2천만 명이 Shibboleth 프로젝트를 사용하고 있음
- Microsoft가 공개한 .NET 프레임워크 3.0은 Indigo라는 개발명으로 알려진 WCF(Windows Communication Foundation)이 포함되어 있음. WCF는 WS-* 스펙을 광범위하게 지원하고 있으므로, .NET 프레임워크 3.0 위에서 자유롭게 WS-* 표준을 사용할 수 있다는 장점이 있음. WCF가 지원하는 WS-* 프로토콜은 Security, reliable messaging, Transaction, Messaging, XML, Metadata 부분임
- Sun은 WS-* 표준을 자바 환경에서도 사용할 수 있도록 오픈소스 커뮤니티를 운영하기 시작. WSIT(Web Services Interoperability Technologies) 프로젝트는 Java 웹서비스와 Microsoft의 WCF 간의 상호호환성을 제공하며, 서비스 중심 아키텍처(SOA)를 쉽게 구축할 수 있게 만들어줌. Security, Reliable Messaging, Atomic Transaction과 같은 주요 기능을 제공. WSIT 오픈소스 구현물은 JAX-WS(Java API for XML Web Services)를 기반으로 함
- Ping Identity는 SAML 1.x와 2.0, WS-Federation을 적용하여 사이트 간의 Federated SSO를 제공하는 PingFederate 4.0을 개발. 또한 WS-Trust 표준을 준용하여 SAML, Kerberos, X.509, ID/PW 등의 토큰을 처리하는 PingTrust 2.0을 2006년 12월에 릴리즈함
- Windows CardSpace는 Microsoft의 최신 운영체제인 Windows Vista에 기본적으로 탑재. .NET 프레임워크 3.0에 포함된 Windows CardSpace는 가입과 로그인 절차를 일관성 있게 유지하며, 피싱 공격을 방지하는 기능을 제공.

또한 .NET 프레임워크 3.0에 포함되어 있는 WCF와 연동되어 있으므로 WS-* 스펙을 자유롭게 활용할 수 있다. Microsoft는 CardSpace 개발 키트를 공개하여 사이트들이 InfoCard를 쉽게 적용할 수 있도록 함

◦ Microsoft의 빌 게이츠는 2007년 2월 초에 개최된 RSA 컨퍼런스에서 CardSpace가 OpenID를 지원하겠다고 발표. Microsoft, JanRain, SXIP, VeriSign 4개 회사가 이들 기술의 상호운용 능력에 대해 공동으로 연구하기로 합의

◦ Microsoft는 2006년 12월 OSP(Open Specification Promise)를 발표하여 MS 소유의 표준 스펙에 대한 특허권을 주장하지 않기로 하였으며, 2007년 5월에는 자사의 CardSpace를 활성화시키기 위하여 4개의 오픈소스 프로젝트를 시작. Sun, Apache Tomcat, IBM, Ruby On Rails, PHP를 타켓으로하고 있으며, 이들 플랫폼에서 쉽게 InfoCard를 사용하는 것이 목적. 초기 결과물은 2007년 7월 초에 릴리즈

◦ 2007년 2월 Ping Identity는 CardSpace 지원 모듈을 제공하여 Apache 서버에서 인증 메커니즘의 하나로 InfoCard를 사용할 수 있도록 함. 또한 2007년 6월 SignOn.com 이라는 사이트를 오픈. 이 사이트는 OpenID 제공자이며, 인증 수단의 하나로 Microsoft CardSpace를 통한 InfoCard를 지원

- 이클립스(Eclipse) 재단에서 운영되는 오픈 소스 프로젝트인 Higgins는 Microsoft의 CardSpace와 같은 ID 메타시스템을 목표로 개발을 진행 중에 있으며, 2006년 2월경부터 IBM과 Novell 등의 업체들로부터 후원을 받고 있음. Higgins 프로젝트는 Novell의 Bandit 프로젝트에서 클라이언트 모듈로 참여하고 있으며, 2007년 3월 개최된 BrainShare 2007에서 상호 연동 작업을 마치고 시연에 성공. 또한 2007년 6월 말에 개최된 Catalyst 2007에서는 Higgins를 비롯한 7개의 Identity Selector와 12개의 IDP, 25개의 RP가 상호호환성 테스트에 참여하여 성공적으로 동작하는 모습을 보여줌

◦ Higgins 프로젝트를 통해 수행된 결과는 2007년 여름 경에 Higgins Trust Framework 1.0으로 발표될 예정

- Sxipper는 Firefox 브라우저의 확장 기능을 이용한 패스워드 관리 어플리케이션으로, WebWare에서 선정한 2007년 100대 웹 소프트웨어임. 개인 데이터는 암호화하여 안전하게 유지하며, 자동 Form Filling 기능을 제공. OpenID 표준을 준용하여 OpenID를 이용한 로그인과 속성 정보 교환, 인증 레벨 정책에 따른 인증 기술을 제공하는 PAPE(Provider Authentication Policy Extension) 스펙 또한 제공

- Password Manager XP(eXtra Protection)는 보안상 중요한 정보를 저장 관리하는 어플리케이션임. 모든 로그인 id, 패스워드, PIN 코드, 신용카드 번호, 접근 코드, 파일, 기타 중요 정보들을 한 곳에 안전하게 저장할 수 있음. Blowfish, 3DES, Rijndael, Tea, Cast128, RC4, Serpent, Twofish 등의 암호화 알고리즘이 지원되어 원하는 암호화 방식을 사용할 수 있으며, 패스워드 생성 기능, 여러 컴퓨터에서 네트워크를 통해 여러 데이터베이스에 접근할 수 있는 기능, 패스워드 데이타베이스를 USB 플래시 드라이브와 같은 착탈식 장치에 저장할 수 있는 기능, 패스워드 데이타베이스의 백업 및 복원기능 등이 제공. 현재 Password Manager XP는 버전 2.2가 공개되어 있음

- P3P는 해당 웹사이트를 방문하지 않고 검색 프로그램을 이용하여, 해당 웹사이트와 자신의 프라이버시 선호 수준을 입력을 하면 정책 선호도 및 해당 웹사이트의 정책 원문을 확인할 수 있는 에이전트의 새로운 대안 프로그램으로 2003년에 AT&T 개발을 시작으로 IBM 등에서 구현되고 있음

◦ 또한, P3P 관련 S/W는 크게 에이전트와 정책생성기, 사업자용과 이용자용으로 나누어 개발되며, 대부분의 S/W는 무료로 보급되고 있으나 정책 생성기는 일부 유료로 제공. 유로 정책 생성 S/W는 Customer Paradigm은 225$

이며, P3Pdeveloper.com에서는 29.95$임

◦ 사업자용 P3P는 IBM Tivoli Privacy Manager, 알파웍스, JRC P3P APPEL Privacy Preference Editor 등이 있고, 이용자용 P3P로는 Netscape 7.0, AT&T Privacy Bird, IE 6.0 등이 개발되어 보급되고 있음

- XACML은 특정 자원에 접근하기 위해 전송되는 요청자의 속성들(예로, SAML assertions, Java permission, WS-Security tokens 등)을 안전한 메커니즘들과 결합시켜 웹 서비스, J2EE 및 다른 전자상거래 환경들의 권한부여 인프라를 구성하게 하는 요소기술로 현재 Parthenon Computing(Jiffy Software), Sun Microsystems, Lagash Systems 등에서 XACML 버전 1.0 및 1.1 제품을 개발하여 호환성 테스트를 진행하고 있는 등 아직 시제품 수준
- 미국의 대표적인 블록암호 알고리즘 DES(Data Encryption Standard)는 1977년 미연방표준 FIPS 46으로 제정. 이후 암호학자들에 의해 DES가 분석되고 이를 대신할 AES(Advanced Encryption Standard)로 Rijndael을 세계적인 공모사업을 통해 채택
- 유럽에서는 전자상거래, 전자정부 및 전자서명 등을 구현하기 위해 필수적 요소인 암호원천기술에 대한 공모사업 NESSIE(New European Schemes for Signatures, Integrity, and Encryption) 프로젝트를 추진
- 일본에서는 전자정부 실현을 위해 민간 주도하에 CRYPTREC 프로젝트를 진행하여 다양한 암호 원천기술을 발굴

〈표 4〉 국외 ID관리 및 접근제어 솔루션 개발 현황

구분	기관	내용
User-centric ID	Microsoft	- 안전하고 신뢰된 방법으로 자신의 디지털 ID를 온라인 서비스에 제공하는 클라이언트 소프트웨어 - 다양한 ID 표준 지원 - 일관된 사용자 컨트롤 지원 - 패스워드 기반의 웹 로그인을 대체하는 토큰 기반의 보안 포맷 제공 - MS의 차세대 OS인 Vista에 탑재되어 제공
	Intel	- personal server - 전통적인 입출력 기능 없이 무선 인터넷을 이용하여 개인정보를 접근할 수 있음 - 인텔의 XScale 마이크로 아키텍처를 기반으로 저전력을 요구하면서 고성능의 연산이 가능함 - Apache 웹서버를 통해 무선으로 웹서비스를 지원하며, 파일 공유, 원격 기기제어 기능을 제공함
	SXIP	- OpenID - URL을 식별자로 사용하는 범용 인증 프로토콜을 제안 - LID, SXIP, SXIP, XRI/i-names 프로토콜을 포함하고 있음 - 지적재산권으로 보호받지만, 누구나 자유롭게 사용할 수 있는 정책임
	NetMesh	- SXIP, lid - LID는 URL을 식별자로 사용하는 인증 프로토콜로 SSO, 프로파일 데이터 교환, 소셜 네트워킹, 인증된 메시징과 블로깅을 제공할 수 있음
	NeuStar	- i-names - 도메인 네임과 유사하게 사람이 읽을 수 있는 식별자지만, 더 간단하고 사용하기 쉬움 - 조직의 경우 '@', 개인의 경우 '=' 가 접두사로 붙는 식별자 정책사용 - 식별자 뒤에 '+' 로 개인정보를 추가하여 공유할 수 있음 - 2006년 6월에 한국을 비롯하여 전세계에 서비스를 런칭하였음
Federated ID	Microsoft	- Active Directory Federation Service - Microsoft 제품 기반에서의 연동으로 시작되었으나, Unix, Linux 플랫폼으로 확장 - 중앙 집중 방식으로 ID관리 및 SSO 제공 - 특정 표준에 국한되지 않고 다양한 ID 기술을 적용한 플랫폼 기술인 ID 메타시스템 개념을 적용함
	Liberty Alliance	- Amex, AOL, GM, HP, Nokia, Sony, Sun 등 약 150 여개 업체로 구성 - 웹 서비스 지원을 위한 표준 제공 - 네트워크 ID 정보에 대한 보안과 개인정보 보호 제공 - 제3의 신뢰 기관 없이 고객 관리 및 연계 가능 - 분산된 인증, 인가를 통한 SSO 제공

구분	기관	내용
I&AM	IBM	- Tivoli Identity Manager - 웹기반의 셀프서비스 인터페이스 - 사용자 요청의 제출 및 승인과정을 자동화해주는 워크플로우 - 관리 작업의 적용을 자동화해주는 프로비저닝 엔진 - 관리자 권한 위임을 위한 Role 기반의 관리 모델
	SUN	- Java System Identity Manager - 빠르고 정확한 자동화 프로비저닝과 동기화 서비스 제공 - 간단한 정책 설정을 통해 규제 감시와 예방 기능 처리 - 수천 개의 id 생성과 업데이트를 수분 이내에 제공 - 99.9%의 가용성 보장
	Netegrity	- SiteMinder, IdentityMinder - 다양한 환경에서 중앙집중적인 정책기반 인증, 인가 관리 - 웹 서비스를 지원하는 정책기반 솔루션 - Role 기반의 권한 제어 기술과 위임 기술 - 웹 어플리케이션 및 기업 시스템에 대한 ID 기반 관리
	Oblix	- NetPoint with COREid, IDLink - SSO를 통한 편리한 웹 접근 관리 방법 제공 - End-to-End 프로비저닝 - 도메인간의 안전한 Federation 제공 - Seamless Enterprise Integration 제공 - 감사 및 리포팅 기능 제공
Privacy	IBM	- Tivoli Privacy Manager - 진보된 P3P 인터페이스 - Privacy 정책관리를 위한 언어 제공 - 개인정보 접근에 대한 모니터링 및 로그 기능 - 자동 리포팅 기능
	Zero Knowledge	- Enterprise Privacy Manager - Privacy 정책 표현을 위한 EPML(Enterprise Privacy Markup Language) - 기존 시스템으로부터 Privacy 정보 추출 방법 - Privacy 정책 분석 기능 제공 - 정책 리포팅 기능

• 전망

- ID관리 분야는 SAML과 Liberty Alliance로 대변되는 연계 ID 분야, CardSpace로 대변되는 Card-based ID 분야, 그리고 OpenID로 대변되는 URL-based ID 분야로 나뉘어져 있음. 각 분야는 독자적인 활용영역을 가지고 있으나, 점차로 타 기술을 적용하는 융합이 활발하게 이루어지는 추세이며 궁극적으로는 사용자에 의한 제어와 사용자에게 더 많은 권한을 부여하는 방향으로 진행 중

  ◦ SAML은 사용자 식별 방식의 하나로 URL과 XRI를 사용할 수 있으며, OpenID를 적용할 수 있음

  ◦ CardSpace는 OpenID의 피싱 취약점을 해결하는 방안으로 고려

  ◦ CardSpace는 SAML 토큰을 인증 방식의 하나로 채택

- IDC의 조사 결과에 따르면 전세계 IAM(Identity and Access Management) 시장은 2007년 33억 달러에서 2011년에는 49억 달러로 연 10.7% 성장할 전망. 또한 플랫폼 별로 조사한 결과에 따르면 Microsoft 윈도우즈 플랫폼이 2007년 11억 달러에서 2011년 20억 달러로 연 40.4% 성장할 전망

- 전자여권과 전자운전면허증과 같이 전세계에서 통용되는 ID카드의 추진 이후, 유럽에서는 전자운전면허증과 사회보장카드를 통합한 EUID를 개발하고 있어 ID카드의 블록화가 예상. 또한 최근 일본과 한국, 중국 등에서 아시아 IC카드의 개발도 논의되고 있으며, 국내에서는 전자주민증과 같은 대형 국가 프로젝트가 단계별로 추진되고 있어 조만간 일반 국민들에게 국제통용, 지역 통용, 국가ID 등이 보급될 것으로 예상

2.4. 표준화 현황 및 전망

• 개요

- 인터넷 환경에서 제공되는 정보보호는 시스템간의 연동과 확장성을 위해 반드시 표준을 준용하여야 함. ID관리 기술에 대한 표준화는 국제적으로 활발히 진행되고 있으나 개인정보 공유 및 보호 기술에 대한 표준화는 아직 초기 단계
- ID관리 분야의 기반기술과 관련하여, W3C는 XML 전자서명, 암호화, 키관리에 대한 표준을 제정하고 있고 일부 표준은 IETF와 공동으로 추진하고 있으며, IETF는 공개키 인증서, 속성인증서, LDAP에 대한 표준을 제정하고 있음
- ID관리와 관련하여, OASIS는 SAML, XACML, SPML, XRI 등의 표준을 제정하고 있으며, Sun을 중심으로 150여개 업체가 연합한 Liberty Alliance와 IBM과 Microsoft를 중심으로 여러 업체가 연합한 WS-I에서 표준화를 진행하고 있음
- 개인정보 보호와 관련하여, W3C의 P3P와 APPEL, OASIS의 XACML, IBM의 EPAL 등의 규격이 제정되고 있음
- 2005년 3월 OASIS는 기존의 ID관리 표준들을 통합 적용한 SAML 버전 2.0을 공표한 뒤 상호호환성 시험(2005.7)을 개최하여 ETRI를 포함한 8개 기업이 호환성 인증을 받았고, ITU-T가 OASIS와 협의를 통해 SG17 WP2 Q.6에서 수행하는 SAML과 XACML의 표준화 작업에 국 · 내외 전문가들이 참여
- ID관리와 관련하여, ISO는 SC17에서 IC카드의 자체 및 응용 분야 기술에 대한 표준을 제정하고 있으며, SC27 WG5에서 ID관리와 프라이버시 기술에 대한 표준을 제정하고 있으며, ID관리와 프라이버시 분야의 향후 표준과 가이드라인을 작성하기 위한 요구 사항과 개발 내용을 도출하는 단계
- 국내의 경우, 한국정보보호진흥원과 한국정보통신기술협회(TTA)가 정보보호 및 전자서명에 대한 표준을 제정하고 있으며, ETRI와 TTA에서 ID관리, 개인정보 보호와 관련하여 SAML 2.0 주장과 프로토콜, 바인딩, 프로파일 표준화 작업을 국내 표준으로 제정(2006.12)

2.4.1. 국내 표준화 현황 및 전망

- 국내 정보보호일반표준은 인터넷보안기술 포럼과 TTA에서 추진. 표준화는 두 가지 방법으로 추진되고 있는데, 한 가지 방법은 사실표준화단체가 표준초안을 개발하고, TTA에서 정보통신 단체표준으로 개발하는 방법이고, 다른 방법은 TTA에서 표준 초안이 개발되고 관련 PG를 통하여 최종 표준을 확정하는 방법으로 표준안을 개발하는 방법
- 국내 개인정보보호 관련 표준화는 표준 기획 단계로, 국외 표준 기구에서 채택된 표준안을 국내 표준으로 추진하는 정도에 머물고 있는 실정
- TTA 정보보호기반 프로젝트 그룹(PG101)
  - TTA에서 개인정보보호 관련 표준화는 TC1 PG101 정보보호기반 프로젝트 그룹에서 주로 논의되고 있으며, XACML v1.0을 바탕으로 XACML 적합성 및 상호호환성 평가 표준을 2004년에 제정하고, 확장성 접근제어 생성

언어(XACML v1.0) 표준을 국제 표준화 기구 ITU-T 표준 제정에 조금 늦은 2006년에 제정

◦ 또한, 2006년 SAML 2.0 주장과 프로토콜, 바인딩, 프로파일에 대한 국내 표준화를 완료하였으며, 2007년에 SAML 2.0 메타데이타, 인증 문맥에 대한 표준화 작업을 진행하여 완료할 예정

◦ 또한, P3P v1.1을 바탕으로 국내 관련 법률을 적용한 개인정보보호정책 설정 및 협상 규격이 표준화 과제로 채택되어 2007년 표준화 채택을 목표로 검토 중에 있음

- 국내 TTA에 확정된 개인정보보호 및 ID관리 관련 표준은 다음과 같음

관련분야	표준번호	표준내용	제정년도	개정현황
PKI 및 인증	TTAS.KO-12.0012	전자서명 인증서 프로파일 표준	2000	제정완료
	TTAS.KO-12.0013	전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준	2001	제정완료
	TTAS.KO-09.0003/R1	부가형 디지털 전자서명방식 - 제1부: 기본구조 및 모델	2005	제정완료
ID관리	TTAS.IT-X1141_1	SAML 2.0 주장과 프로토콜	2006	제정완료
	TTAS.IT-X1141_2	SAML 2.0 바인딩	2006	제정완료
	TTAS.IT-X1141_3	SAML 2.0 프로파일	2006	제정완료

2.4.2. 국외 표준화 현황 및 전망

- ITU-T SG17 FG IdM(Focus Group on Identity Management)에서는 포괄적인 IdM 프레임워크 개발을 촉진하고 분산 환경에서 자율적인 ID 발견, ID 연계 및 구현 수단 개발을 진행. FG IdM 외에도 ITU-T에는 ID관리와 관련된 Study Group들이 있는데 Q.15/13(NGN Security)에서는 NGN(Next Generation Network) 환경에서 보안 요구사항 권고안을 확정하였고 인증, AAA, 보안 메커니즘, NGN 인증서, IdM 보안 등에 관한 권고 초안을 개발 중. 그리고 A.6/17(Cybersecurity)에서 작성 중인 X.IdM(IdM Security)에 관한 권고안이 ID관리 시스템과 관련이 깊고 중요
- ISO에서 ID관리와 연관된 표준화 활동들로는 인터넷 기반 PKI에 대한 ISO 9594-8(X.509 PKI 인증서 및 인증서 취소 목록, IETF RFC 3280과 관련), 전자 거래(electronic transaction)에서 활용되는 전자 ID에 대한 명세 ISO/IEC 15944-1(Information technology - Business agreement semantic descriptive techniques - Part 1: Operational aspects of Open-Electronic Data Interchange(EDI)), 생체인식정보 교환 표준형식을 개발하는 ISO/IEC 19794, ID관리 프레임워크를 연구하는 ISO/IEC JTC1 SC27(Information Technology - Security Techniques - A Framework for Identity Management) 등이 있음. SC27 WG5에서는 ID 개념, ID, 식별(identification) 및 식별자(identifier), ID 생명주기, ID 인증, 정보사회에서 ID관리, 정보기술과 ID관리, 정보보안과 ID관리 등 포괄적인 ID관리에 대한 표준 개발을 진행. 또한 전자여권과 관련하여 ISO/IEC JTC1 SC17 WG3, 전자운전면허증과 관련하여 ISO/IEC JTC1 SC17 WG10, 바이오 카드와 관련하여 ISO/IEC JTC1 SC17 WG11 등이 표준 개발을 진행
- IETF에서 개발된 표준 중 ID관리와 연관된 RFC들로는 자원이나 개체 식별을 위한 RFC3986(Uniform Resource Identifier), URI를 포함하는 식별자에 대한 표준들인 RFC3987(Internationalized Resource Identifier),

RFC2822(Internet Message Format), RFC2141(Uniform Resource Name), RFC4122(Universally Unique Identifier, Globally Unique Identifier), RFC4474(Enhancements and Authenticated Identity Management in the Session Initiation Protocol), RFC4484(Trait-Based Authorization Requirements for the Session Initiation Protocol) 등이 있음

- W3C에서는 ID관리와 관련된 XML 권고안들을 개발하였는데 대표적인 예로는 XML 문서의 ID 속성인 xml:id 의미를 정의하는 xml:id Version 1.0, 웹 정보 및 프로토콜 메시지 부분에 대한 전자서명 규격을 정의하는 XML Signature WG의 권고안, XML 문서 전체 및 부분에 대한 암호/복호 절차, 암호화된 부분 지정 및 정당한 수신자가 복호화할 수 있는 정보 지정을 위한 XML 문법을 정의하는 XML Encryption WG의 권고안, 공개키 등록 및 분배 프로토콜을 정의하는 XKMS(XML Key Management Specification) 등이 있음
- OASIS에서 제정한 ID 관련 표준들로는 SAML, XACML, SPML, XRI, WS-Security(Web Service Security) 등이 있음. SAML 표준에서는 주체에 대해 발행된 assertion 구조 및 assertion 처리를 위한 관련 프로토콜들에 대해 정의하고 있으며 XACML은 정보시스템에 의해 관리되는 자원에 대한 접근허용여부를 정의하는 XML 언어 기반 보안정책 기술언어 표준임. SPML은 사용자, 자원, 서비스 프로비저닝 정보교환을 위한 XML 기반 프레임워크를 정의하고 있으며 XRI는 위치, 응용, 전송 프로토콜과 독립적인 URI와 호환성있는 추상적 식별자와 결정(resolution) 프로토콜에 대한 표준을 정의하고 있음. WS-Security 표준에서는 웹 서비스 메시징에 적용되는 무결성 및 비밀성 지원을 위한 프로토콜을 정의하고 있음
- OMA(Open Mobile Alliance)는 멀티벤더 환경에서 응용과 서비스를 효과적이고 안정적으로 구축, 설치, 관리하도록 하는 공개형 표준기반 프레임워크를 개발하여 가입자에게 시장, 사업자, 그리고 모바일 단말기 등에 걸쳐 상호호환 가능한 모바일 서비스를 제공함을 목표. OMA에 의해 개발된 IdM 관련 명세로는 ID Management Framework Requirement(OMA-RD-Identity_Management_Framework-V1_0-20050202-C)가 있음. 이 명세의 목적은 모든 OMA enabler들에 의해 공통적으로 사용될 수 있는 단일 IdM enabler를 만드는 데 있으며 이 명세에는 모든 OMA 기술 WG들의 요구사항들과 단일 IdM enabler가 제공해야 하는 ID관리 관련 모든 기능들을 포함되어 있음
- 3GPP는 전 세계적으로 적용가능한 제3세대 이동통신망 표준개발을 목표로 유럽의 ETSI(European Telecommunications Standards Institute), 일본의 ARIB/TTC(Association of Radio Industries and Businesses/Telecommunication Technology Committee), 중국의 CCSA(China Communications Standards Association), 북아메리카의 ATIS(Alliance for Telecommunications Industry Solutions), 그리고 한국의 TTA(Telecommunications Technology Association) 협력 하에 1998년 결성된 ITU IMT-2000 국제 표준화 기구임. 3GPP가 유럽 주도의 DS(Direct Sequence) 방식의 비동기식 제3세대 이동통신망 표준화 단체인데 비해 3GPP-2는 미국 주도의 동기식 제3세대 이동통신망 표준화 단체임
- Liberty Alliance project는 연계 ID관리를 위한 가이드라인과 실례 그리고 공개 표준을 개발할 목적으로 2001년에 결성되었고, 웹 서비스의 소비자들이 ID 정보에 대한 프라이버시와 보안을 유지하면서 온라인 업무를 어디에서든지 더 쉽게 할 수 있게 하는 것을 목표. ID들이 연계되어 연결되고, 공유함으로써 사용자에게 SSO, Single Logout 등의 편리함을 제공. Liberty Alliance project는 크게 세 개의 모듈로 구성되어 있다. 여러 사이트의 사용자 계정을 연결

하는 ID의 연계를 다루는 ID-FF, ID서비스의 생성, 검색, 사용을 위한 프레임워크를 제공하는 ID-WSF와 ID-WSF 위에서 일정, 주소록, 달력, 위치추적, 사용자 상태나 경고등을 위한 ID 기반의 서비스를 다루는 ID-SIS로 구성되어 있음

- OASIS는 E-business 와 웹 서비스의 공통 표준들을 개발하는 것이 목표로 진행. OASIS의 기술적 영역은 웹서비스, 전자상거래, 보안, 법률과 정부, 컴퓨터 관리 등이다. OASIS에서 명세한 표준으로는 CAP(Common Alerting Protocol), CIQ(Customer Information Quality), DocBook, DITA(Darwin Information Typing Architecture), OpenDocument(OASIS Open Document Format for Office Application), SAML, SPML, UBL(Universal Business Language), WSDM(Web Services Distributed Management), XRI, XDI 등이 있음. 이중 XRI는 인터넷 규모의 URI 기반 추상화된 ID를 정의하는 명세와 XRI 데이터 공유를 위한 조율 프로토콜, 도메인 상호간에 자원 공유 등을 명세하고 있음. 또한 XDI는 XRI에 기반을 둔 dataweb 구축을 목표로 인터넷 규모의 멀티 도메인들 간에 XRI와 XDI 기본 스키마에 기반을 둔 XML 도큐먼트를 상호간에 서로 공유하고 링킹, 동기화하는 표준화를 제안하고 있음
- 개인정보보호 및 ID관리 관련 국제 표준은 다음과 같음

표준화기관	표준식별자	제목
Liberty Alliance	liberty-idff-bindings-profiles	Liberty ID-FF Bindings and Profiles Specification V1.2
	liberty-idff-protocols-schema	Liberty ID-FF Protocols and Schema Specification V1.2
	liberty-idwsf-disco-svc	Liberty ID-WSF Discovery Service Specification V2.0
	liberty-idwsf-soap-binding	Liberty ID-WSF SOAP Binding Specification V2.0
	liberty-idwsf-security-mechanisms	Liberty ID-WSF Security Mechanisms Specification V2.0
	liberty-idwsf-interaction-svc	Liberty ID-WSF Interaction Service Specification V2.0
	liberty-idwsf-client-profiles	Liberty ID-WSF Client Profiles Specification V2.0
	liberty-idwsf-dst	Liberty ID-WSF Data Service Template Specification V2.1
	liberty-idwsf-authn-svc	Liberty ID-WSF Authentication Service Specification V2.0
	liberty-idwsf-people-service	Liberty ID-WSF People Service Specification V1.0
	liberty-idwsf-subs	Liberty ID-WSF Subscription and Notification Specification V1.0
	liberty-idsis-pp	Liberty ID-SIS Personal Profile Service Specification V1.1
	liberty-idsis-ep	Liberty ID-SIS Employee Profile Service Specification V1.1
	liberty-idsis-sis-cb	Liberty ID-SIS Contact Book Service Specification V1.0
	liberty-idsis-sis-gl	Liberty ID-SIS Geolocation Service Specification V1.0
	liberty-idsis-sis-presence	Liberty ID-SIS Presence Service Specification V1.0
OASIS	oasis-sstc-saml-core-1.1	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1
	oasis-sstc-saml-bindings-1.1	Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1
	oasis-sstc-saml-conform-1.1	Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML) V1.1
	sstc-saml-core-2.0-os	Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0
	sstc-saml-bindings-2.0-os	Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0
	sstc-saml-profiles-2.0-os	Profiles for the OASIS Security Assertion Makrup Language (SAML) V2.0

표준화기관	표준식별자	제목
OASIS	sstc-saml-metadata-2.0-os	Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0
	sstc-saml-authn-context-2.0-os	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0
	oasis-xacml-2.0	Hierarchical resource profile of XACML V2.0
	oasis-xacml-2.0	Multiple resource profile of XACML V2.0
	oasis-xacml-2.0	Privacy policy profile of XACML V2.0
	oasis-xacml-2.0	SAML 2.0 profile of XACML V2.0
	oasis-xacml-2.0	XML Digital Signature profile of XACML V2.0
	os-pstc-spml2-dsml-profile-os	Service Provisioning Markup Language (SPML) V2.0 - DSML V2 Profile
	os-pstc-spml2-xsd-profile-os	Service Provisioning Markup Language (SPML) V.02 - XSD Profile
	os-pstc-spml-cd-2.0	Service Provisioning Markup Language (SPML) V2.0
	xri-syntax-v2.0-cd-01	XRI Syntax V2.0 Committee Draft 01
	xri-resolution-v2.0-cd-01	XRI Resolution V2.0 Committee Draft 01
	xri-metadata-v2.0-cd-01	XRI Metadata V2.0 Committee Draft 01
IETF	RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
	RFC 3281	An Internet Attribute Certificate Profile for Authorization
	RFC 3377	Lightweight Directory Access Protocol(v3) : Technical Specification
W3C, IETF	xmldsig-core/RFC3275	XML-Signature Syntax and Processing
W3C	P3P 1.1	The Platform for Privacy Preferences 1.1 (P3P1.1) Specification
	APPEL1.0	A P3P Preference Exchange Language 1.0 (APPEL1.0)
	EPAL 1.2	Enterprise Privacy Authorization Language (EPAL 1.2)
	xmlenc-core	XML Encryption Syntax and Processing
	xmlenc-decrypt	Decryption Transform for XML Signature
	xkms 2.0	XML Key Management Specification (XKMS) Version 2.0
	soap v 1.2 Spec	SOAP Version 1.2 Part 1, 2

2.5. 표준화 대상항목별 현황 분석표

표준화 대상항목		ID관리 프레임워크	개인정보보호
시장 현황 및 전망	국내	- 한국 IDC에 따르면 ID관리 및 접근제어 시장 규모는 2005년 238억 원에서 연평균 12% 성장하여 2009년 425억에 이를 것으로 전망하고 있음	
	국외	- IDC에 따르면 ID관리 및 접근제어 시장 규모는 2005년 25억 달러에서 연평균 11.3% 성장하여 2009년 40억 달러에 이를 것으로 전망하고 있음	
기술 개발 현황 및 전망	국내	- ETRI에서 보안토큰 생성 · 분배, 디스커버리 ID 연계 기술 개발 보유 - SSO, EAM 시스템 제품군 출시 - OpenID, XRI 식별체계를 지원하는 제품군 출시 - ID 공유 기술 연구중 - PKI, 메타데이타를 통한 시스템간의 신뢰관리기술 보유	- ETRI에서 XACML 기술과 Interaction Service 기술 개발 - Data Protection Audit 기술은 EAM, I&AM 제품의 기능으로 포함됨 - IC카드를 이용한 ID의 보급이 추진되고 있으므로, IC카드를 이용한 개인정보보호 기술이 요구됨
	국외	- 식별체계, 보안토큰 생성 · 분배, 디스커버리 등 핵심 기술이 다수 개발된 상태임 - SSO, EAM 등 개별 기능 제품군에서 ID를 종합적으로 관리하는 I&AM 제품군이 다수 출시됨 - 최근 User-Centric 제품군이 출시되고 있음 - PKI, 메타데이타를 통한 시스템간의 신뢰관리기술	- P3P, XACML 기술 개발됨 - Liberty에서 Interaction Service 기술 개발 - Data Protection Audit 기술은 EAM, I&AM 제품의 기능으로 포함됨 - 전자여권, 전자운전면허증 등 국제통용 ID의 보급이 추진되고 있음
기술 개발 수준	국내	기술기획-상용화	기술기획-시제품
	국외	시제품-상용화	시제품-상용화
	기술격차	1년	1~2년
	관련제품	PKI, EAM, I&AM	PKI, EAM, I&AM
IPR 보유현황	국내	-	-
	국외	-	-
IPR확보 가능분야		프레임워크, 디스커버리, ID Sharing	개인정보보호정책, Data Protection Audit
IPR확보 가능성		부분 선도	부분 선도
표준화 현황 및 전망		- 국제 표준화 단체들에서 부분 기술에 대한 표준 개발이 진행되고 있으며, 국내에서는 Security Token에 대한 표준 개발이 진행되고 있음	- Interaction Service에 대한 표준이 Liberty Alliance에서 개발되었으며, 개인정보보호정책에 대한 표준이 OASIS에서 개발되었으며, 국내 표준 개발은 아직 미흡한 상태임 - 서비스 자체에 대한 표준화는 부분적으로 완료된 것으로 볼 수 있으나, 해당 서비스 내에서 개인정보 보호부분은 지속적인 연구가 필요함
표준화 기구/ 단체	국내	TTA	TTA / ECIF / 기술표준원
	국외	ITU-T SG17, OASIS, Liberty Alliance	ISO, OASIS, Liberty Alliance
	국내참여 업체 및 기관현황	TTA, ETRI 등	TTA, ETRI, KISA 등
	국내기여도	높음	높음
표준화 수준	국내	표준기획 - 표준개발/검토	표준기획
	국외	표준안 개발/검토 - 표준안 최종검토	표준안 개발/검토 - 표준 개발
국내표준화의 인프라수준 (시장요구정도 및 참여도)		높음	높음

표준화 대상항목		ID관리 응용 및 기타
시장 현황 및 전망	국내	- 한국 IDC에 따르면 ID관리 및 접근제어 시장 규모는 2005년 238억 원에서 연평균 12% 성장하여 2009년 425억 원에 이를 것으로 전망하고 있음
	국외	- IDC에 따르면 ID관리 및 접근제어 시장 규모는 2005년 25억 달러에서 연평균 11.3% 성장하여 2009년 40억 달러에 이를 것으로 전망하고 있음
기술 개발 현황 및 전망	국내	- KISA에서 i-PIN 기술을 개발하여 온라인주민번호 대체 서비스 실시 중 - 네트워크 중심 ID관리 기술 연구중 - XML 전자서명 및 암호화 기술은 정보보호제품 전반에 적용되고 있음
	국외	- OMA와 3GPP 표준 개발 - XML 전자서명 및 암호화 기술은 정보보호제품 전반에 적용되고 있음
기술 개발 수준	국내	상용화
	국외	상용화
	기술격차	없음
	관련제품	정보보호 제품 전반, Portal
IPR 보유현황	국내	-
	국외	-
IPR확보 가능분야		i-PIN
IPR확보 가능성		선도
표준화 현황 및 전망		- i-PIN은 국내 표준이 제정되어 있으며, XML 전자서명 및 암호화 기술은 국럼뼁騈岵막 표준이 개발되어 있는 상태임
표준화 기구/ 단체	국내	TTA
	국외	ITU-T, OASIS, Liberty Alliance, OMA, 3GPP
	국내참여 업체 및 기관현황	TTA, ETRI, KISA 등
	국내기여도	높음
표준화 수준	국내	표준제정
	국외	표준기획 - 표준제정
국내표준화의 인프라수준 (시장요구정도 및 참여도)		높음

3. 중점 표준화항목의 표준화 추진전략

3.1. 중점기술의 표준화 환경분석

3.1.1. 표준화 추진상의 문제점 및 현안사항

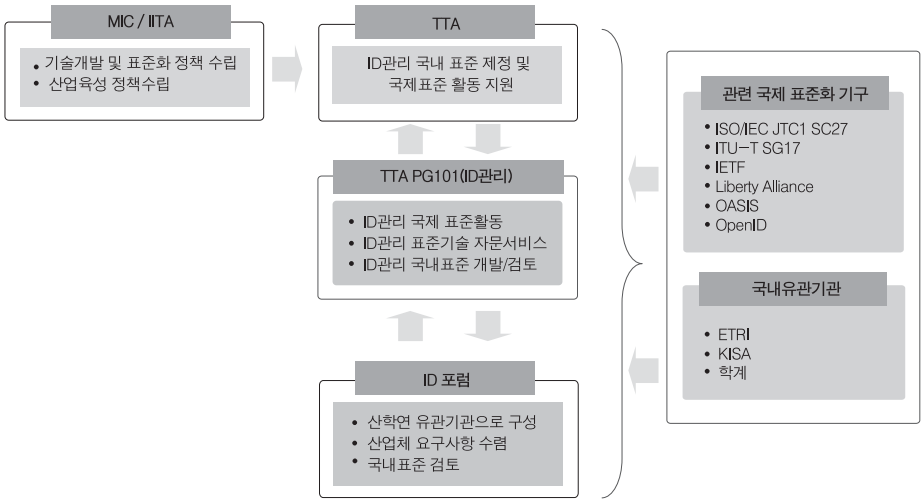
- 인터넷 상에서의 ID 도용 및 개인정보유출 문제는 이전부터 존재해 왔으나, 인터넷에 기반을 둔 전자상거래와 전자정부가 활성화되고 있는 최근에야 문제의 심각성이 일반인에게 인지되고 사회적인 문제로 인지되고 있는 상황
- 현재 ID관리에 대한 표준화를 진행하고 있는 국제단체는 ITU-T SG17과 ISO/IEC JCT1/SC27이 있으며, 이들 단체에서는 최근에서야 ID관리에 대한 표준화를 진행. 따라서 ID관리 기술에 대한 핵심 기술을 개발하고 우수 핵심 기술을 국제 표준화 단체의 표준으로 채택하도록 하여 많은 IPR을 확보하기에는 현재가 적기
- 국내에서는 현재 ID관리 표준이 주로 TTA의 정보보호기반 프로젝트 그룹인 PG101에서 표준화가 진행되고 있다. 그러나 표준화가 주로 ETRI, KISA 등과 같은 연구기관과 학계를 통해 이루어지고 있으며 산업체의 참여가 상대적으로 저조하기 때문에, ID관리 기술에 대한 통신사 및 중요 포털을 포함하는 산업계의 요구가 수렴될 수 있는 ID 관련 포럼이 결성되어 국내 표준화 활동이 활성화되는 것이 필요
- 개인정보를 보호하기 위한 기술들은 국가별, 지역별, 환경별로 각기 다른 정책이나 법률, 지침 등이 적용 가능해야하며 변경이 자유로워야 하는 특성을 갖고 있어 설정된 수준을 객관적으로 판단할 수 있는 일반화된 기준을 규정하기 어렵고, 공통적으로 적용할 수 있는 기술을 개발하거나 표준화하는데 어려움이 있다. 향후 이용자 중심의 환경을 고려한 개인정보보호 기술 개발이 필요

3.1.2. SWOT 분석 및 표준화 추진방향

국내역량요인 / 국외환경요인			강점 요인 (S)	약점 요인 (W)
		시장	- 정보통신 인프라구축이 잘 되어 있고, 새로운 기술 수용이 매우 빠름 - 정통부 i-PIN, 행자부 통합ID관리서비스 등 ID관리에 대한 국가 인프라 구축의지	- 정보보호 시장 규모의 상대적 협소 - 정보보호 산업체의 영세성, 브랜드 인지도 부족으로 경제성 형성의 한계 - 정보보호 구축에 많은 비용이 소요되나 투자 대비 회수 비용의 산정이 매우 어려움
		기술	- 정부의 확고한 지원 정책(IT839) 추진으로 인한 새로운 정보보호 서비스와 새로운 정보보호 장치 개발의 필요성 대두 - ETRI를 통한 선도 기술개발을 통한 핵심 기술 확보 가능	- 기술개발 고급 인력 부족 - 정보보호 기능이 구현되는 플랫폼 기술이 전무하여, 응용 위주의 제품 생산
		표준	- 국제표준화 활동에 조기참여 및 대응 - 정부의 강력한 IT 분야의 국제표준전문가 양성 프로그램 시행	- 정보보호 표준 전문가의 부족 - 업체의 표준 추진 의지 미흡 - 행정편의성 증진 등의 사유로 개인정보 보호에 다소 소극적임
기회요인 (O)	시장	- ID 도용과 개인정보 유출 피해 증가에 따른 ID관리 기술에 대한 관심 고조 - ID관리 분야의 시장 규모가 급속히 증가될 예정임 - 국가적 차원 및 국제통용 ID의 발급 추진	- 개인정보보호 및 ID관리 분야의 국내 독자 IPR 확보 - ITU-T/SG17, ISO/IEC JTC1/SC27 등 국제표준화 기구에서의 표준화 활동 강화 - ETRI 등의 국책 연구기관에서 개발된 선도 개발기술의 국제 표준화 추진	- 신규 ID 서비스에 대한 시장 창출을 통한 지속적인 정보보호 인력 양성 - 공공 분야의 ID 인프라 구축 및 개인정보보호 제품 확대를 통한 국내 정보보호 시장 확대 - 지속적인 기반 기술 개발과 우수 제품 개발을 통해 국내 정보보호 수준 제고 및 제품 경쟁력 향상 - ID관련 포럼 등의 설립을 통해 국내 산업계의 요구사항을 수렴하고 PG101을 통해 국내 표준화를 수행 - IC카드 활용 ID 시스템에서 개인정보보호 기술 적용
	기술	- 웹2.0의 등장 등의 외부 환경변화에 따라 ID관리 및 개인정보보호 관련 핵심 기술 개발 필요성 증가		
	표준	- ID관리 관련 국제표준화가 ITU-T와 ISO에서 초기 단계이기 때문에, 국제 표준화 참여 및 선도 가능		
위협요인 (T)	시장	- 미국, 유럽 등 ID관리 제품을 제공하는 기업들의 독점 우려 - 개인정보보호의 경우 국가별 정책, 규제 등과 일치시켜야 하는 문제 발생	- 개발된 ID관리 기술을 국내의 인터넷 환경에 선적용하여 제품의 인지도와 완성도를 제고하여 해외 시장 경쟁력을 확보 - 개인정보보호 및 ID관리 관련 국외 연구기관과 전문가 초청 워크숍을 통한 기술 교류 - TTA PG101을 통해 국내 표준화를 수행하고 국책연구기관의 표준전문가를 적극 활용하여 국제표준화 추진	- 선도기반 과제를 통한 IPR 획득 및 이를 통한 기술 및 서비스 제공 - 산 · 학 · 연 연계 연구 개발을 통해 지속적인 정보보호 고급 인력을 양성하고 이를 통해 기반 기술 확보 - 투자비 환수의 개념을 탈피한 ID 도용 및 개인정보 분야의 유출의 피해 예방 개념을 적용한 정책적 지원을 통한 정보보호 제품 구매 확대 정책 시행 - 정보 집중화로 인하여 빅브라더 우려에 대한 개인의 ID 통제권 부여 등 적극적 개인정보 보호 기술 적용
	기술	- 국외 일부 국가와 회사에서 핵심 원천기술에 대한 기술적 우위 선점		
	표준	- 국가간, 업체간 경쟁이 치열 - 선진국의 경우 국제표준 경험 및 전문 인력 풍부 - 국가주의에 의한 개인정보 보호에 대한 우려		

SO전략 : 공격적 전략(강점사용-기회활용) / WO전략 : 만회전략(약점극복-기회활용) / ST전략 : 다각화 전략(강점사용-위협회피) / WT전략 : 방어적 전략(약점최소화-위협회피)

3.1.3. 표준화 추진체계



〈그림 4〉 개인정보보호 및 ID관리 기술의 표준화 추진체계

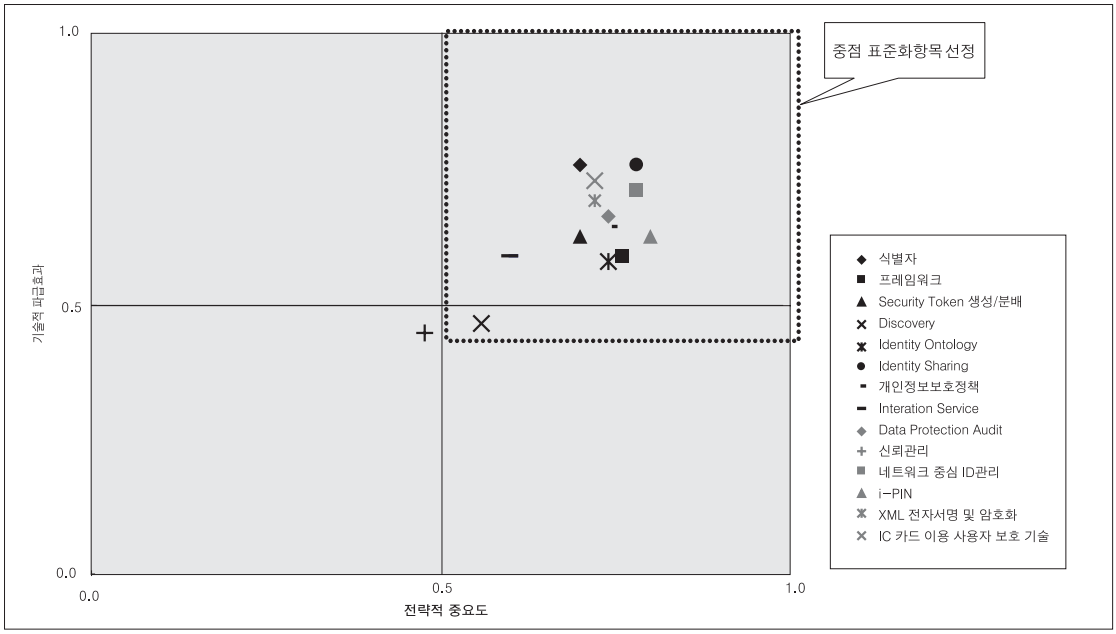
- 국내 표준은 ETRI, KISA 그리고 정보보호 산업체에서 국내 표준 초안을 개발하고 TTA를 통하여 정보통신 단체 표준으로 개발한다. 정보통신 단체 표준은 TTA TC1 PG101을 통하여 추진
- ID관리와 개인정보보호 기술을 집중적으로 다루는 ID관리 포럼을 국내 산업계, 학계, 연구기관으로 구성하여 학계의 기반 기술과 산업계의 요구사항을 ID 포럼 등을 통해 수렴할 수 있도록 하며, 개발된 국내 표준을 검토
- ISO/IEC JTC1과 ITU-T에 국내 표준 전문가들이 활발히 참여하여, 국내에서 개발된 개인정보보호 및 ID관리 기술에 대한 국제 표준화를 수행

3.2. 중점 표준화항목 선정

3.2.1. 중점 표준화항목 선정방법

표준화 대상항목별 전략적 중요도 및 기술적 파급효과 분석												
	전략적 중요도						기술적 파급효과					
고려요소	P_1 산학연 관심도 (투자 등)	P_2 정부 관심도 (정책 등)	P_3 표준선도 가능성 (표준 투자정도)	P_4 표준(기술)개발의 시급성	P_5 기술(표준) 격차	PI (Priority Index)	E_1 타 산업 파급효과	E_2 경제적 파급효과	E_3 국내외 시장규모	E_4 IPR확보 가능성 (로얄티 수입)	E_5 사용자편의 (호환성/공공성 등)	EI (Effect Index)
고려요소별 가중치(합계 1)	0.1	0.3	0.3	0.2	0.1	1	0.2	0.2	0.1	0.3	0.3	1
식별자	3.0	4.0	4.0	3.0	2.0	0.7	4.0	4.0	3.0	4.0	4.0	0.8
프레임워크	3.0	4.0	4.0	4.0	3.0	0.8	3.0	3.0	3.0	3.0	3.0	0.6
Security Token 생성/분배	4.0	4.0	3.0	4.0	2.0	0.7	4.0	4.0	4.0	2.0	3.0	0.6
Discovery	3.0	2.0	3.0	4.0	2.0	0.6	3.0	3.0	2.0	2.0	2.0	0.5
Identity Ontology	3.0	4.0	4.0	4.0	2.0	0.7	3.0	3.0	2.0	2.0	4.0	0.6
Identity Sharing	4.0	4.0	4.0	4.0	3.0	0.8	4.0	4.0	3.0	4.0	4.0	0.8
개인정보보호정책	3.0	4.0	3.0	4.0	3.0	0.7	4.0	4.0	3.0	2.0	4.0	0.7
Interation Service	4.0	3.0	3.0	3.0	2.0	0.6	3.0	3.0	3.0	3.0	3.0	0.6
Data Protecttion Audit	4.0	5.0	3.0	3.0	3.0	0.7	4.0	4.0	3.0	2.0	4.0	0.7
신뢰관리	3.0	2.0	3.0	2.0	2.0	0.5	2.0	2.0	2.0	3.0	2.0	0.5
네트워크 중심 ID관리	4.0	3.0	5.0	4.0	3.0	0.8	4.0	4.0	3.0	3.0	4.0	0.7
i-PIN	3.0	5.0	4.0	4.0	2.0	0.8	4.0	3.0	3.0	2.0	4.0	0.6
XML전자서명 및 암호화	3.0	3.0	4.0	4.0	4.0	0.7	3.0	3.0	3.0	4.0	4.0	0.7
IC카드 이용 사용자 보호 기술	3.0	3.0	4.0	4.0	4.0	0.7	4.0	4.0	4.0	3.0	4.0	0.8

* 표준화 대상항목의 각 고려요소별 평가점수는 해당 중점기술의 전문기술 의견을 종합하여 산출함.
* 각 고려요소별 평가점수는 1(매우낮음) - 2(낮음) - 3(보통) - 4(높음) - 5(매우 높음)의 5점 척도임.



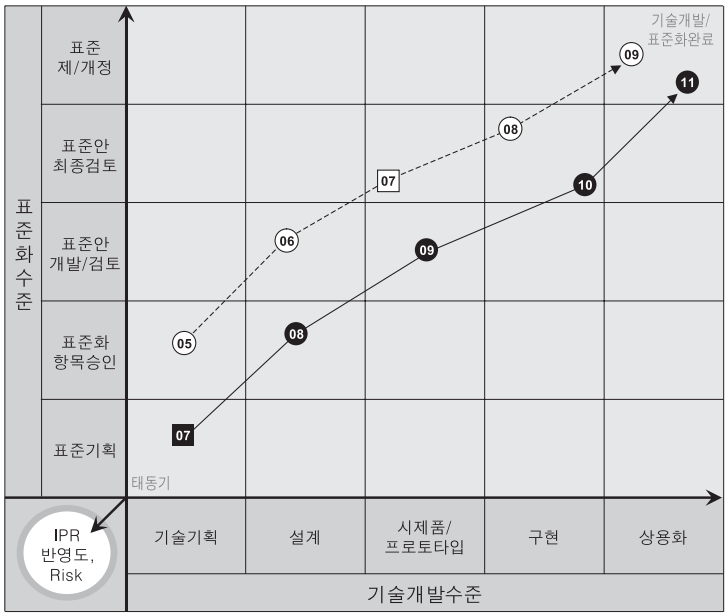
3.2.2. 중점 표준화항목 선정사유

- ID관리와 개인정보보호 분야의 표준화 항목 중에서 전략적 중요도와 기술적 파급효과가 모두 0.5보다 큰 분야를 2008년도 개인정보보호 및 ID관리 분야의 중점 표준화 항목으로 선정
- 프레임워크, ID Sharing, 네트워크 중심 ID관리는 전략적 중요도가 매우 큰 분야이며, 특히 네트워크 중심 ID 는 국제적으로 통신망의 진화와 관련한 핵심 표준화 분야로 부각되고 있는 분야여서, 조기 선점을 위한 표준화 연구개발의 필요성이 큼
- 식별자와 ID Ontology, 프레임워크는 ID관리와 개인정보보호의 기반이 되는 것으로 ID 분야의 기반 요소로 기술적 파급효과가 매우 큰 분야임
- Security Token 생성/분배, Discovery는 ID관리 시스템 운용의 핵심 요소 기술로 ID관리의 필수 핵심 분야임
- 개인정보보호정책과 Interaction Service는 개인정보를 보호하는 정책을 설정하고 판단하며, 개인정보 제공시 사용자의 동의 여부를 확인하고, 개인정보 유출시 책임 소재를 확인할 수 있도록 하는 기능을 제공하는 등 개인정보보호 서비스를 위한 필수 분야임
- i-PIN과 Data Protection Audit은 정부 정책 의지가 매우 큰 분야이며, 특히 i-PIN의 경우 온라인상에서의 신원확인 용도를 위해 필수적인 분야임
- IC카드 이용 사용자 보호 기술은 향후 이용자 중심 환경 구축을 위하여 필수적인 분야이며, 기술규격 완성시 국제표준으로 추진도 가능한 분야임

3.3. 중점 표준화항목별 세부전략(안)

3.3.1. 식별자

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA ID 포럼	ETRI KISA	IETF OASIS

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

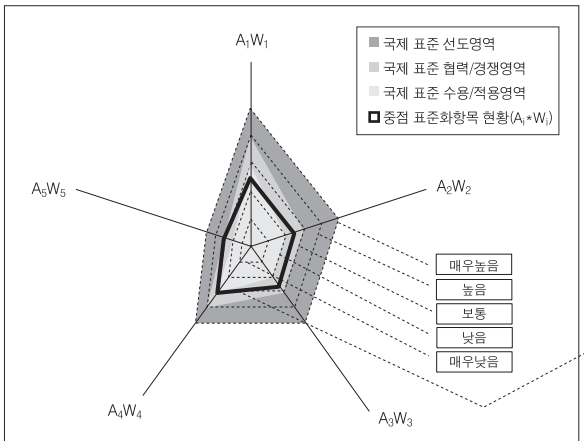
--→ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

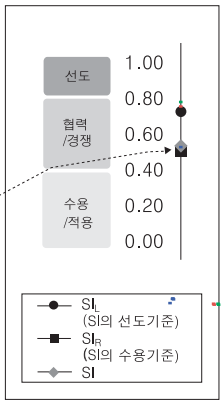
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.53



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

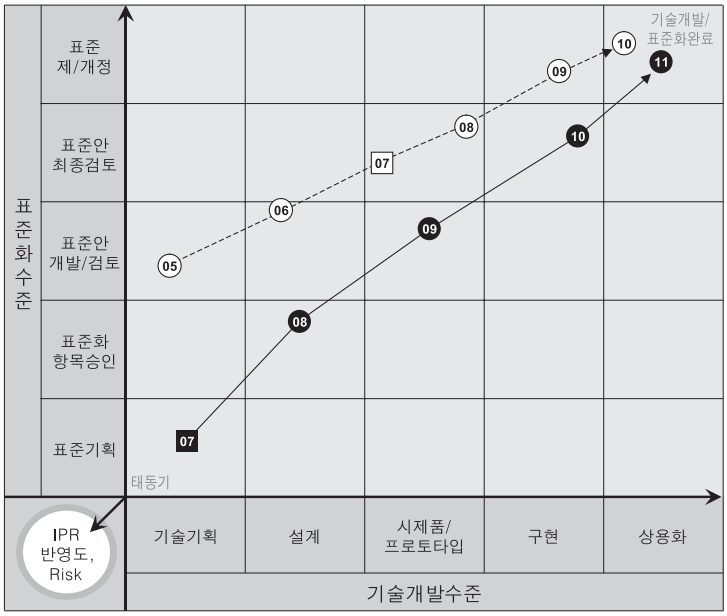
국제표준수용/적용 [일부 협력/경쟁]

- 세부전략(안)

  - 현재 IETF 1738 URL 표준은 TTA 국내 표준으로 수용되어 있는 상태
  - 전세계 인터넷 자원을 유니코드로 동일하게 식별할 수 있는 IETF RFC 3986 URI 표준의 국내 수용이 요구됨
  - ID 자원에 대한 식별자로 현재 개발이 진행되고 있는 OASIS의 XRI 2.0을 수용하여 국내 표준화 작업을 수행하는 것이 요구됨

3.3.2. 프레임워크

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID 포럼	ETRI KISA	ISO Liberty

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

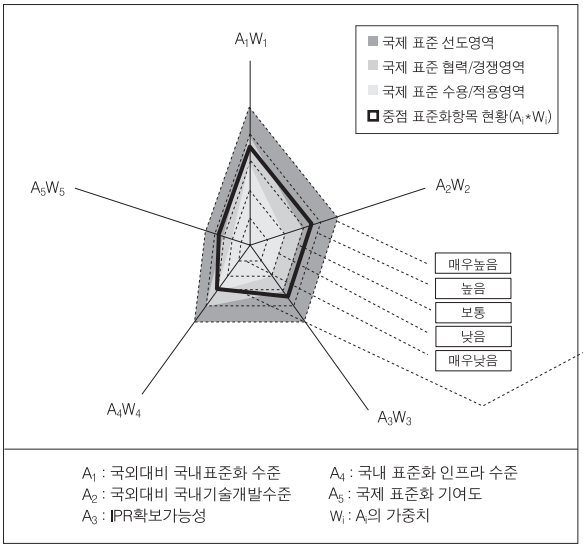
-→ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

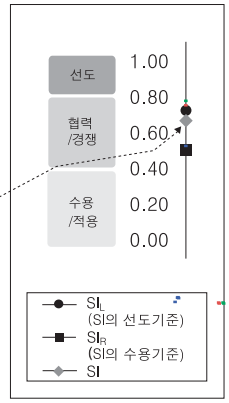
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.68



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$

$$(0 < W_i < 1, 0 < SI \leq 1)$$

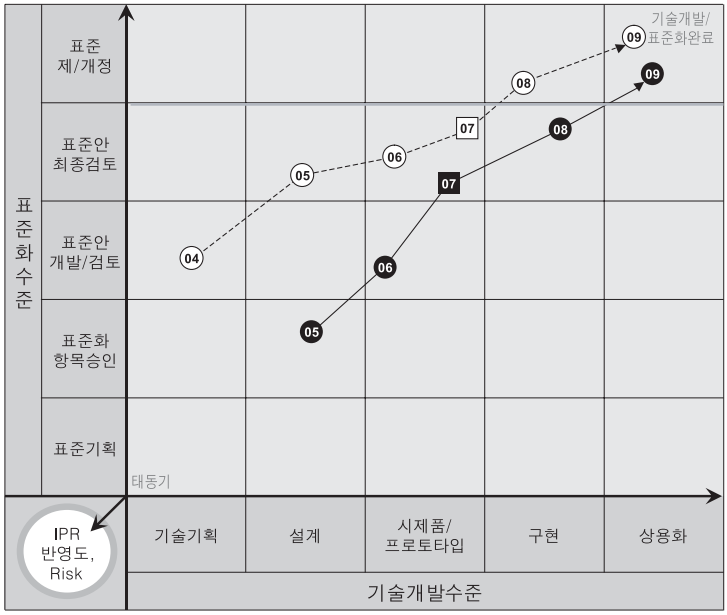
국제표준 선도

• 세부전략(안)

- Liberty Alliance에서 ID 프레임워크로 개발한 ID-WSF 2.0을 산업계 표준을 제정한 상태
- ISO의 SC27에서는 ID관리 기술에 대한 프레임워크 표준화를 제정 중
- ITU-T SG17에서는 ID관리 기술 Focus 그룹을 2007년부터 운용하여 Global Interoperable ID관리 프레임워크에 대한 표준을 제정 중
- 국내에서는 Liberty Alliance의 ID-WSF와 ISO, ITU-T 표준화 진행을 참고하고, ID-WSF 개발 경험을 토대로 국내 환경에 적합한 ID관리 프레임워크 표준을 제정하는 것이 필요함
- 또한, ITU-T SG17의 지속적인 국제 표준화 활동을 통해 국내에서 개발되는 ID 프레임워크 기술을 국제 표준으로 반영되도록 하여 국제 표준을 선도하는 것이 필요함

3.3.3. Security Token 생성/분배

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID 포럼	ETRI	ITU-T OASIS

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

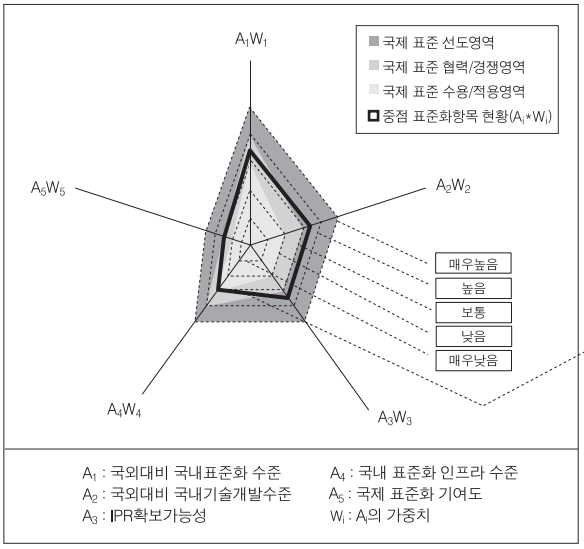
- → : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

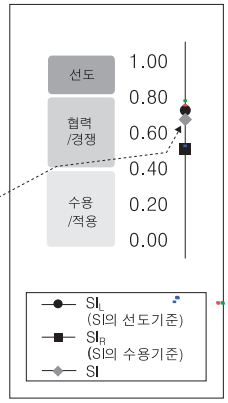
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.67



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

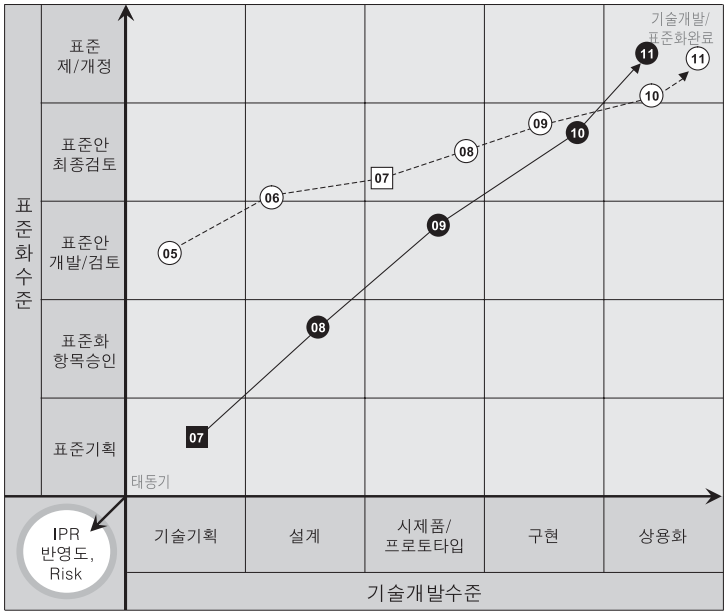
국제표준 선도 [일부 수용/적용]

• 세부전략(안)

- ITU-T의 X.1141 “Security Assertion Markup Language (SAML 2.0),” 표준 중에서 SAML 2.0 Assertion and Protocol, SAML 2.0 Binding과 SAML 2.0 Profile 부분은 2006년 현재 TTA 표준으로 수용된 상태이고, 2007년도 현재, SAML 2.0 Metadata, SAML 2.0 Authentication Context와 SAML 2.0 Conformance Requirements와 Privacy Considerations 부분이 TTA 표준으로 제정 중인 상태
- ID관리에서 필요한 Security Token 구조에 대한 연구를 통해 국내 표준을 생성하고 이를 ITU-T의 기고문을 통하여 국제 표준화하는 노력이 필요함
- 다양한 ID관리 프레임워크에 공통적으로 사용될 수 있는 Uniform Identify Transfer Token과 서로 다른 Security Token을 해석하여 교환할 수 있는 Token Transformation 기술을 개발하여 국제 표준을 선도하는 것이 필요함

3.3.4. Discovery

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID 포럼	ETRI	Liberty OpenID

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

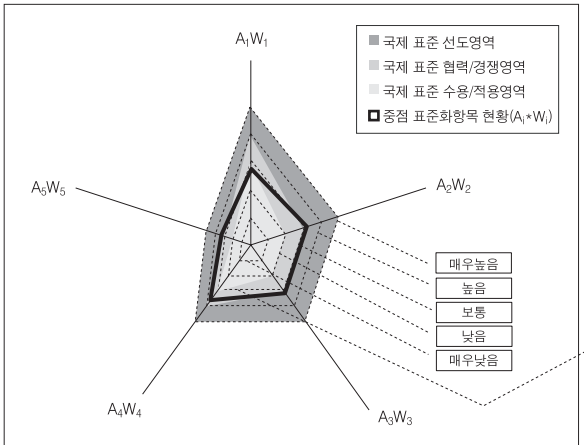
⇢ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

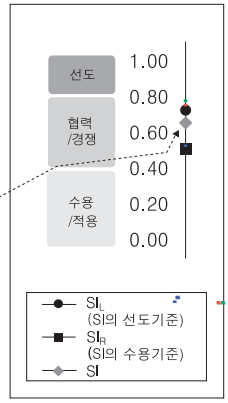
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.64



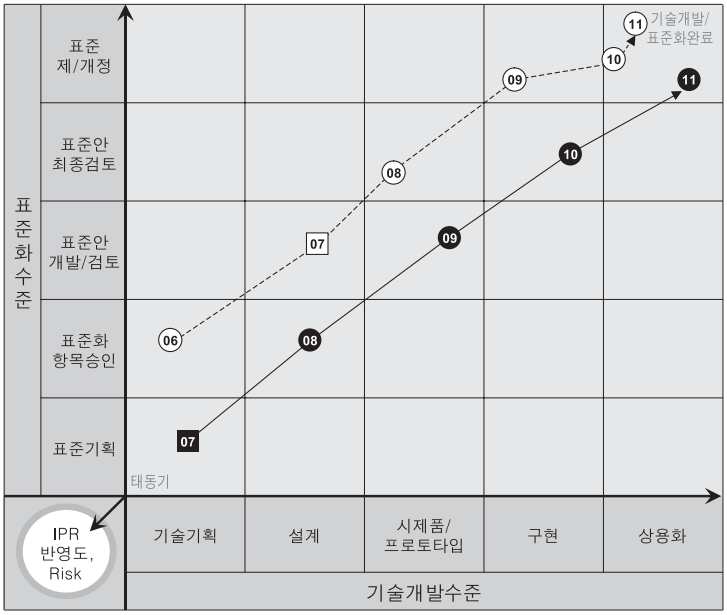
$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

국제표준 선도 [일부 수용/적용]

- 세부전략(안)
  - Liberty Alliance에서 Discovery 표준으로 ID-WSF discovery Service Specification을 산업계 표준을 제정한 상태
  - OpenID에서는 Open Standard의 일환으로 SXIP Project를 진행하여 ID 검색 기술을 개발 중
  - 국내에서는 Liberty Alliance의 ID-WSF Discovery Service Specification과 SXIP 개발 기술을 참고하고, 국내 환경에 적합한 ID discovery 표준을 제정하는 것이 필요함
  - 다중 도메인에서 상호호환이 가능한 discovery 기술을 개발하여 국제 표준화 단체에 기고하여 국제 표준을 선도하는 것이 필요함

3.3.5. ID Ontology

• 표준상태전이도 (표준화 & 기술개발 연계분석)

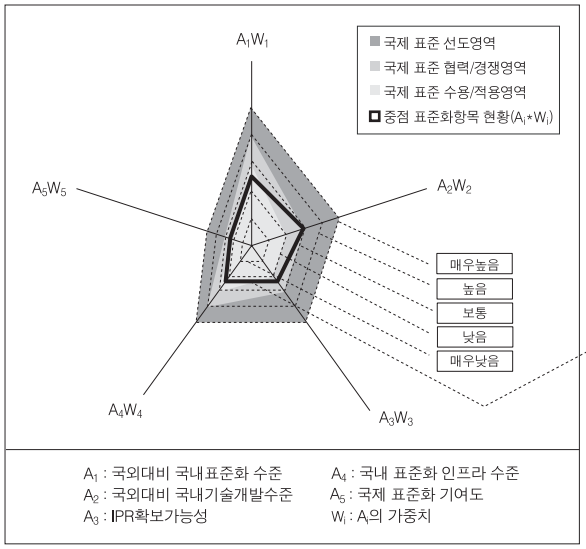


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA ID 포럼	ETRI	ISO W3C OASIS Liberty

범 례

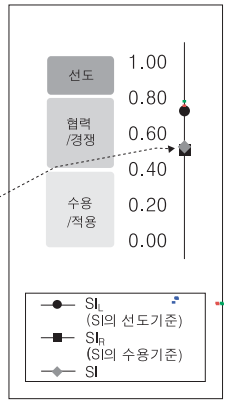
- 07 : 중점 표준화항목의 국내상태
- 07 : 중점 표준화항목의 국제상태
- → : 중점 표준화항목의 국내 표준상태전이
- --→ : 중점 표준화항목의 국제 표준상태전이
- ↑ : 선행표준(선 표준화 후 기술개발)
- ↗ : 동시표준(표준화&기술개발 동시추진)
- ↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화 수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
A_4 : 국내 표준화 인프라 수준
A_5 : 국제 표준화 기여도
W_i : A_i의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.52



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

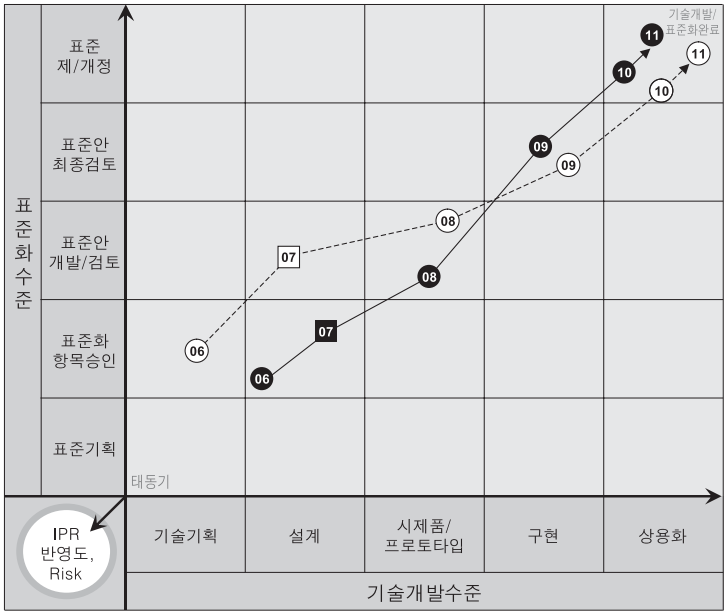
국제표준 수용/적용 [일부 협력/경쟁]

• 세부전략(안)

- ISO/IEC JTC 1/SC27에서 진행 중인 ID관리 프레임워크 표준안 (WD 24760)에 포함된 ID 모델을 참조, 수용하여 국내환경에 적합한 ID Ontology 표준을 개발함
- W3C에서 제정한 웹 환경에서 자원에 대한 정보를 표현하는 체계인 RDF와 웹 온톨로지 정의 및 기술 언어인 OWL을 이용하여 정부 및 기업에서 활용할 수 있는 상호호환성이 보장되는 ID Ontology를 개발
- 현재 ITU-T SG17내 ID관리 Focus Group에서 작성 중인 ID 프레임워크에 ID 모델이나 Ontology에 대해 구체적인 항목이 포함될 경우 해당 내용을 표준 개발과정에 반영함
- OASIS, Liberty Alliance (ID-SIS PP, EP) 등 국외에서 개발된 ID Ontology 표준을 수용하면서 국내환경에 맞는 표준을 개발하는 것이 필요함
- 유럽에서 진행 중인 PRIME 프로젝트 중간 결과로 발표된 ID Ontology의 국내 환경 적용가능성, 표준화 기술 사용여부 등을 판단하여 ID 표준개발 작업에 참조함
- ID Ontology는 사용자 ID에 대한 동일한 뷰 제공, 다양한 종류의 ID관리 시스템간 상호호환성 보장, 개인정보에 대한 프라이버시 정책언어 정의 등 작업에 필요한 핵심적인 선행 표준항목이므로 국제표준을 수용하면서 국내 환경에 적합한 표준개발을 추진함

3.3.6. ID Sharing

• 표준상태전이도 (표준화 & 기술개발 연계분석)

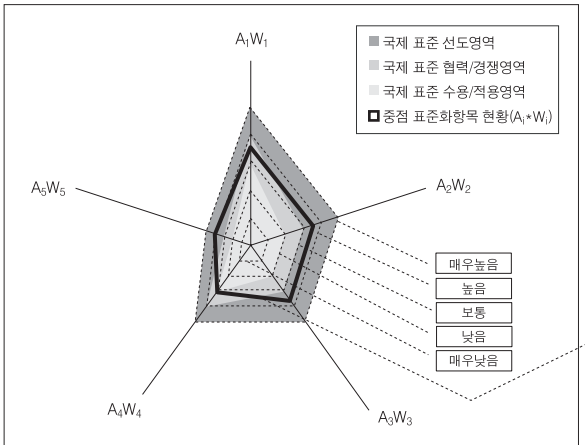


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA ID 포럼	ETRI	ITU-T OASIS Liberty

범 례

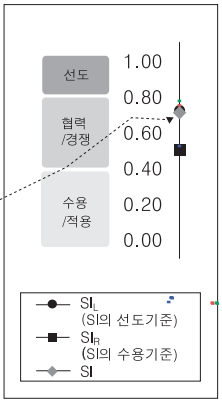
07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화 수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
A_4 : 국내 표준화 인프라 수준
A_5 : 국제 표준화 기여도
W_i : A_i의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.69



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

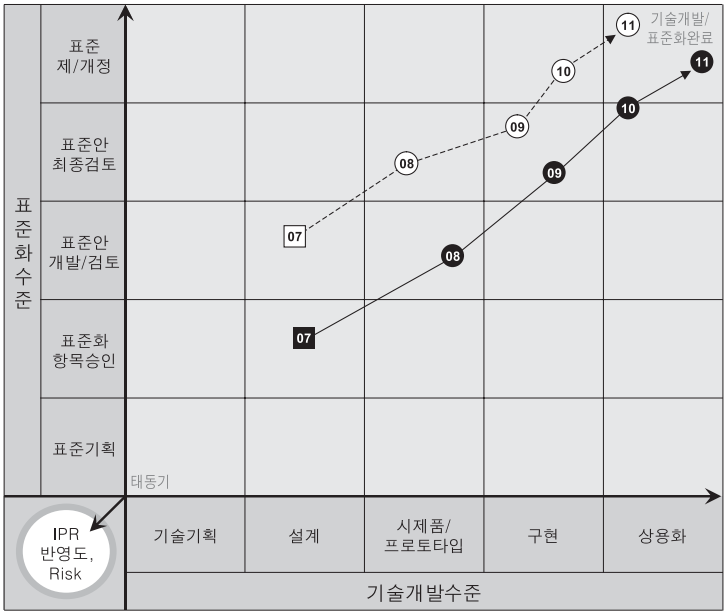
국제표준 선도 [일부 수용/적용]

- 세부전략(안)

- ID 정보 교환을 위한 Liberty Alliance의 ID-WSF, OASIS의 XDI 표준을 참조하고, ID-WSF 기반 인터넷 환경의 ID 공유 및 교환 서비스 개발경험을 토대로 국제 표준 제/개정 작업을 선도함
- ITU-T SG17내 ID관리 Focus Group에서 진행 중인 교환 및 공유 기능에 대한 표준 항목을 고려하여 ID 공유 기능 요구사항 표준작업에 반영함
- 산업체에서 개발된 주요 ID관리 시스템인 Microsoft CardSpace의 ID 교환 프로토콜, OpenID의 Attribute Exchange 프로토콜 특성을 고려하여 ID 공유 요구사항, 관련 프로토콜 표준을 개발함
- 현재 국내에서 개발하고 있는 사용자 중심의 ID Sharing 기술을 ITU-T SG17에 기고하여 국제 표준을 선도하는 것이 필요함

3.3.7. 개인정보보호정책

- 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI KISA	ITU-T W3C OASIS

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

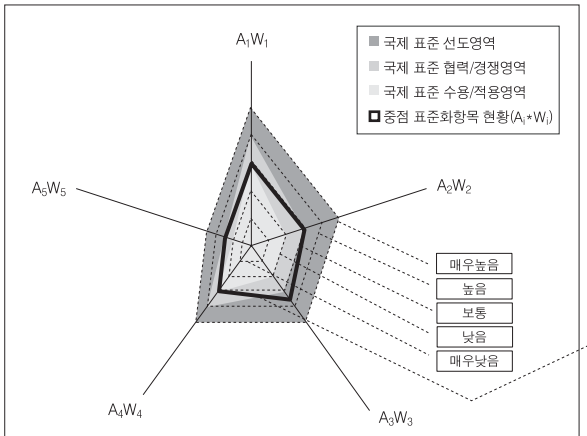
⇢ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

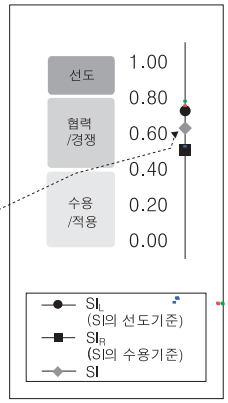
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.62



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

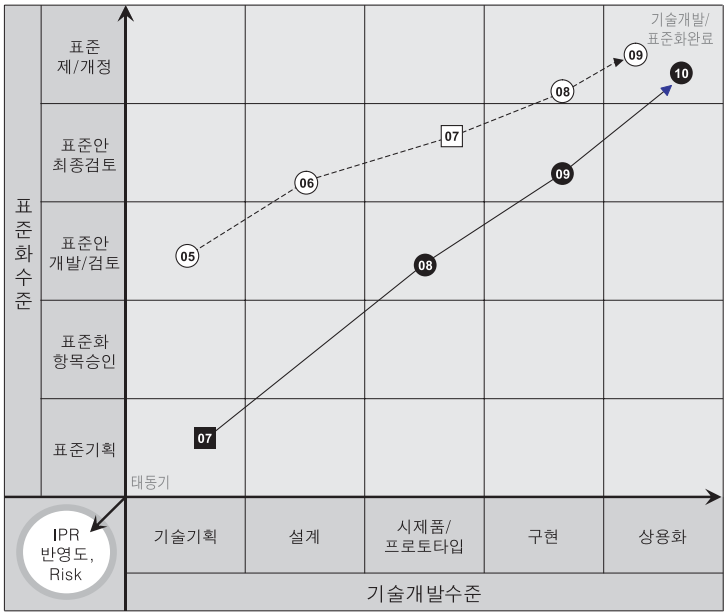
국제표준 선도 [일부 수용/적용]

• 세부전략(안)

- W3C에서는 P3P(Platform for Privacy Preferences) 1.0 표준을 2002년도에 제정하였고 2006년도에는 V1.1 표준을 제정한 상태이며, 국내에서는 TTA에서 2004년도에 P3P 1.0을 수용하여 표준을 제정
- OASIS XACML TC에서는 2003년에 XACML 1.0 표준을 제정하였고, 2005년에는 2.0 버전의 표준을 제정한 상태이며, 국내에서는 2005년 XACML 1.0 버전이 수용되어 국내 표준으로 제정된 상태
- 최신 버전인 W3C의 P3P 1.1과 OASIS XACML 2.0을 국내 환경에 맞게 수용한 국내 표준 개발이 필요함
- 사용자 중심의 개인보호정책에 대한 표준안을 개발하여 ITU-T 등과 같은 국제 표준화 단체에 기고하여 국제 표준화를 선도하는 것이 필요함

3.3.8. Interaction Service

• 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	KISA ETRI	Liberty

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

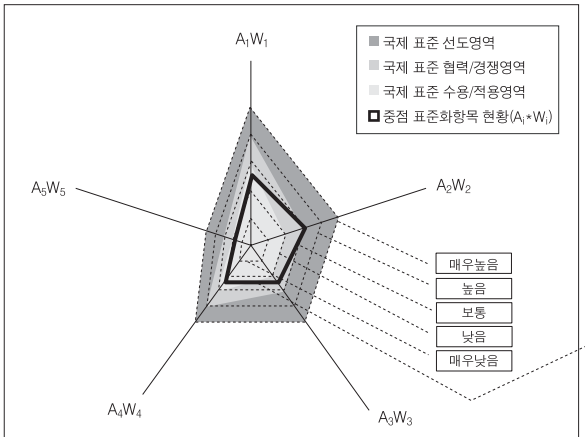
⇢ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

↗ : 동시표준(표준화&기술개발 동시추진)

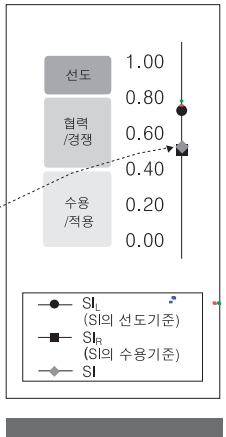
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화 수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
A_4 : 국내 표준화 인프라 수준
A_5 : 국제 표준화 기여도
W_i : Ai의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.51



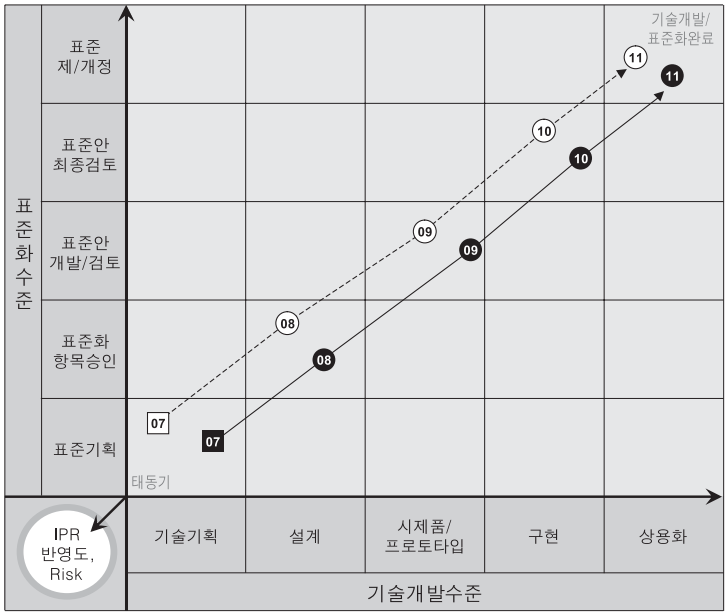
$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

국제표준 수용/적용

- 세부전략(안)
  - Liberty Alliance에서 interaction service 표준으로 2005년도에 ID-WSF Interaction Service 2.0을 제정한 상태
  - Liberty Alliance의 ID-WSF Interaction Service 2.0 표준을 국내 실정에 맞게 수용하는 것이 필요함

3.3.9. Data Protection Audit

- 표준상태전이도 (표준화 & 기술개발 연계분석)

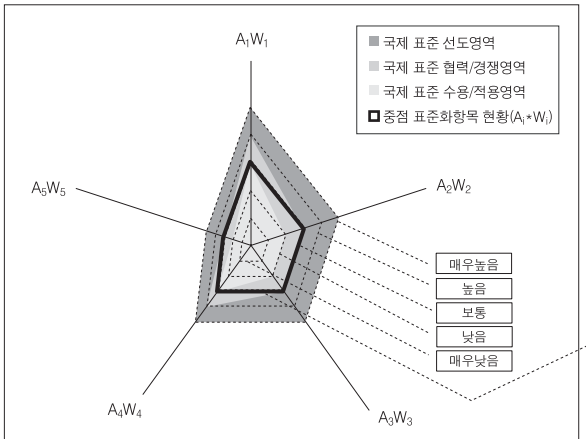


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	KISA ETRI	ITU-T

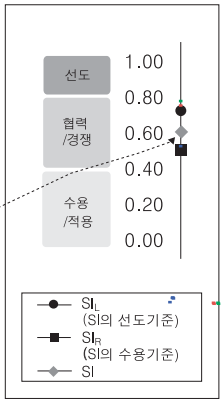
범 례

07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.60



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

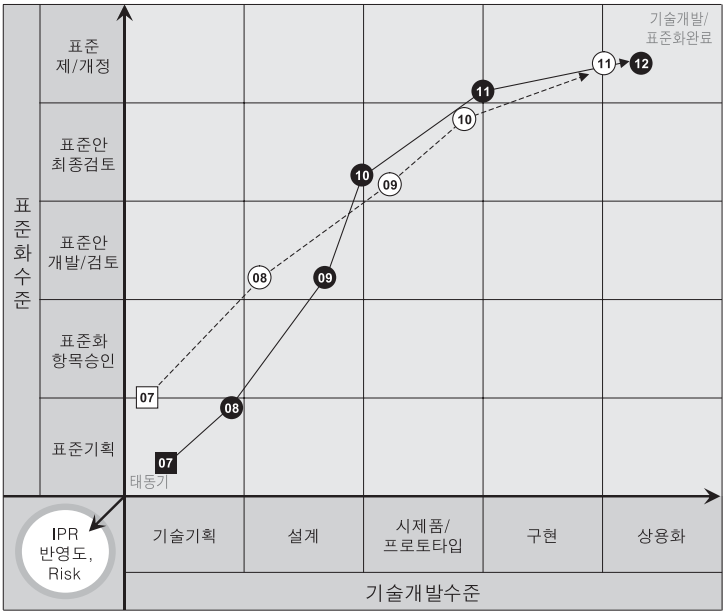
국제표준 수용/적용 [일부 협력/경쟁]

• 세부전략(안)

- ID관리 데이터 보호 및 감사는 개별 제품군에 기능으로 포함되어 있으며 표준화는 국 · 내외적으로 미비한 상황
- 향후, 제품간 상호호환과 데이터 연동의 필요성이 지속적으로 증대될 것으로 예상되며, 이에 따라 국내 표준화 활동을 강화하여 자체적인 표준 개발을 통해 국제 표준화를 선도하는 것이 필요함

3.3.10. 네트워크 중심 ID관리

- 표준상태전이도 (표준화 & 기술개발 연계분석)

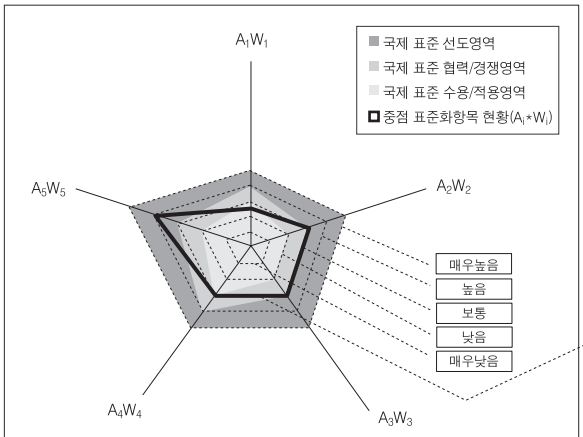


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	TTA	ETRI	ITU-T 3GPP

범 례

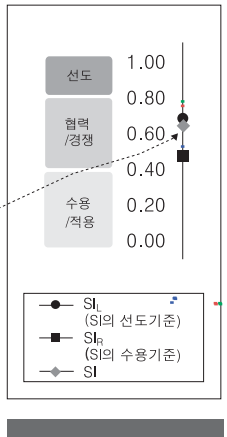
- 07 : 중점 표준화항목의 국내상태
- 07 : 중점 표준화항목의 국제상태
- → : 중점 표준화항목의 국내 표준상태전이
- -→ : 중점 표준화항목의 국제 표준상태전이
- ↑ : 선행표준(선 표준화 후 기술개발)
- ↗ : 동시표준(표준화&기술개발 동시추진)
- ↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



A1 : 국외대비 국내표준화 수준
A2 : 국외대비 국내기술개발수준
A3 : IPR확보가능성
A4 : 국내 표준화 인프라 수준
A5 : 국제 표준화 기여도
Wi : Ai의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.67
SI_R (SI의 수용기준)	0.47
SI	0.64



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

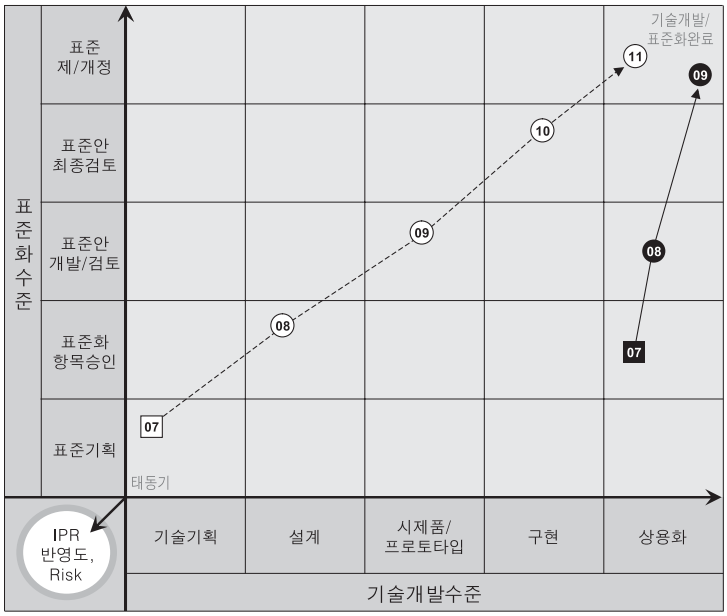
국제표준 선도 (협력/경쟁)

• 세부전략(안)

- ITU-T IDM FG 의 결과문서에 기반하여, 향후 ITU-T에서 ID 관리에 관한 표준화 작업이 활성화 될 것이며, 이들의 작업은 분명하게 NACF (Network Attachment Control Function) 을 주된 작업영역으로 지적하고 있음. 국내에서 ETRI 가 주도하고 있는 ITU-T SG11 의 Q.7 은 Network Attachment 기능 블록을 담당하고 있는 Question 으로, 한국이 주도 하고 있으므로, 이를 기반으로 한 표준화 작업의 진행이 용이한 상태
- 특히 IdM FG 의 주력 멤버들이 NACF 및 Q.7/11 에 대한 우호적인 제스쳐를 보여 오고 있으며, 국내 ETRI에서 Q.7/11 을 담당하고 있는 라포터는 SG2 의 번호체계에 대한 연구도 병행 하고 있어, IdM FG 의 주력 멤버들에게 관심을 끌고 있는 등, 향후 무난한 표준화 주도가 가능하므로, 오히려 이를 통해 입력할 한국 고유의 IPR 개발을 시급히 추진할 예정
- 관련한 Frame work 부문에 대해서는 국제적인 기술의 리더십이 강하며, Verisign, Neustar 등의 영향력과 기술력이 크나, 이에 대해서는 ITU-T SG2 의 활동 배경을 업고, 통신망 중심입장에서 경쟁력 강화를 추진
- 3GPP에서는 GAA(Generic Authentication Architecture)와 GAA와 GBA(Generic Bootstrapping Architecture) 표준을 제정한 상태임
- 국내에서는 3GPP의 표준안들을 기반으로 모바일환경에서의 클라이언트와 서버간의 상호인증 문제들을 해결하는 표준안을 개발하는 것이 필요하며, 이를 바탕으로 국제 표준을 선도하는 것이 필요함
- 또한, IP 기반의 환경적 요인 및 Web 기반의 서비스 구조에 적응하려는 NGN/BcN 의 특성에 맞도록 Liberty Alliance의 ID-FF 등 single-sign-on 기술 구조를 도입하여 GAA/GBA와 통합하는 구조와 시나리오를 갖는 표준을 개발하는 것이 필요함

3.3.11. i-PIN

• 표준상태전이도 (표준화 & 기술개발 연계분석)

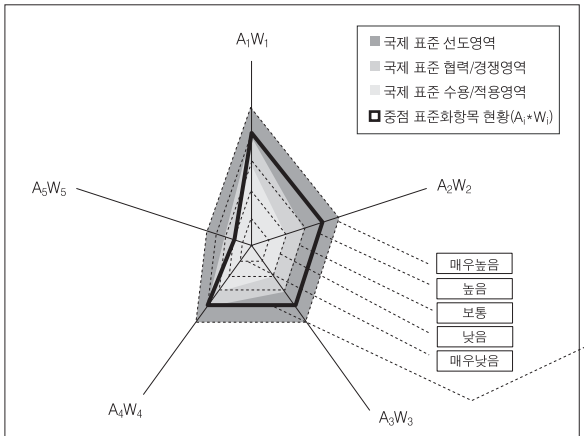


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	KISA	ITU-T

범 례

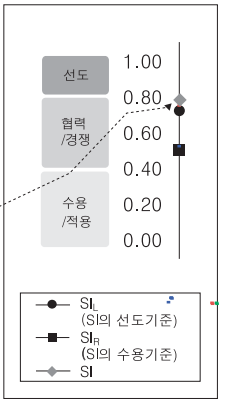
07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

• 국제표준화 전략목표 도출



A_1 : 국외대비 국내표준화 수준
A_2 : 국외대비 국내기술개발수준
A_3 : IPR확보가능성
A_4 : 국내 표준화 인프라 수준
A_5 : 국제 표준화 기여도
W_i : A_i의 가중치

SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.76



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

국제표준 선도

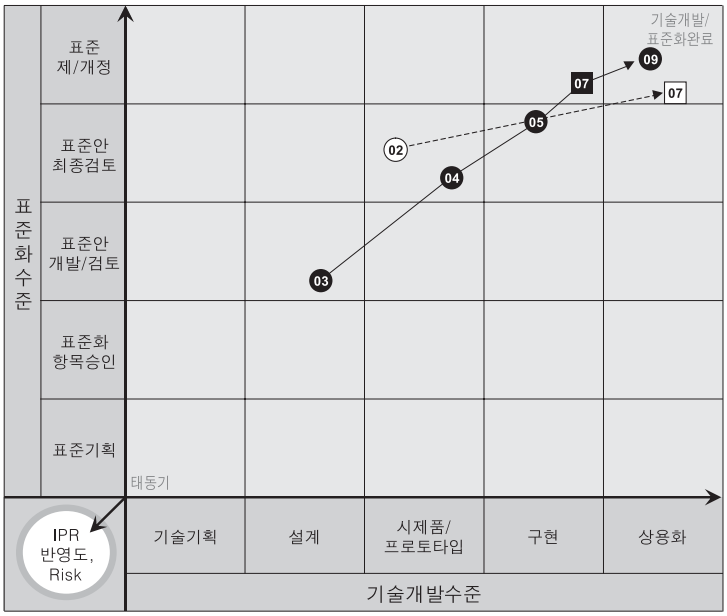
- 세부전략(안)

  - 2007년 현재 i-PIN 표준은 TTA에서 i-PIN 서비스 프레임워크와 i-PIN 서비스 전달 메시지 형식에 대한 표준화가 진행되고 있는 상태

  - i-PIN의 국내 표준화를 빠른 시일 내에 완료하고, 국제 환경에 맞는 규격을 개발하여 ITU-T에 기고하여 국제 표준화를 선도하는 것이 필요함

3.3.12. XML 전자서명 및 암호화

- 표준상태전이도 (표준화 & 기술개발 연계분석)



표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★	TTA	KISA	W3C IETF

범 례

07 : 중점 표준화항목의 국내상태

07 : 중점 표준화항목의 국제상태

→ : 중점 표준화항목의 국내 표준상태전이

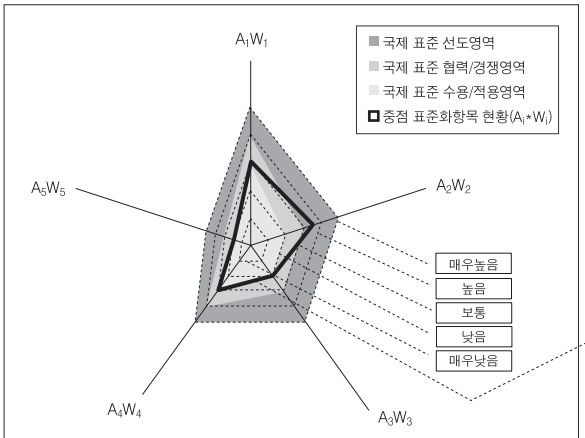
⇢ : 중점 표준화항목의 국제 표준상태전이

↑ : 선행표준(선 표준화 후 기술개발)

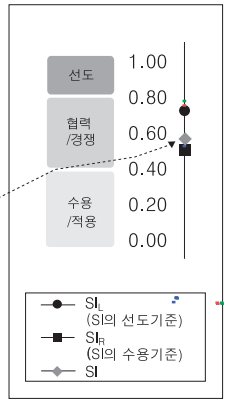
↗ : 동시표준(표준화&기술개발 동시추진)

↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.56



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

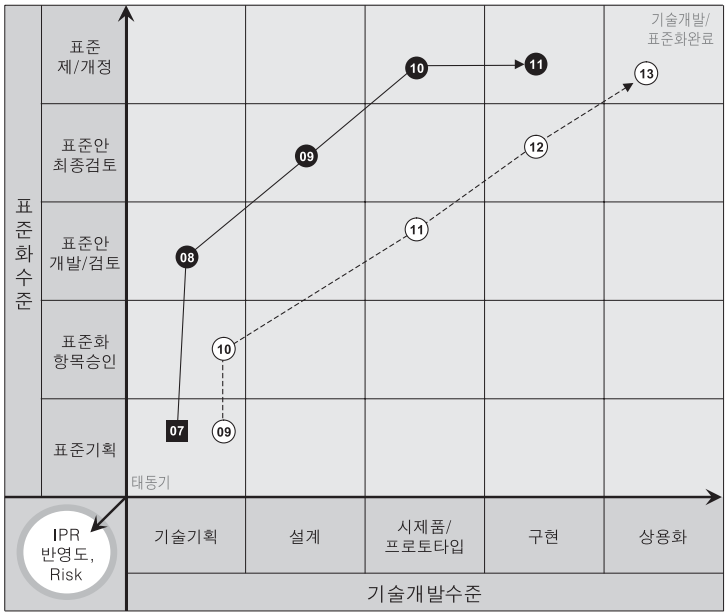
국제표준 수용/적용 [일부 협력/경쟁]

- 세부전략(안)

  - XML 전자서명에 대한 표준화는 W3C에서 2002년에 XML Signature Syntax and Processing으로 국제 표준이 제정된 상태이며, 국내에서도 수용되어 2004년 TTA에서 표준으로 제정된 상태
  - XML 암호화에 대한 표준화는 W3C에서 2002년에 XML Encryption Syntax and Processing으로 국제 표준이 제정된 상태이며, 국내에서도 수용되어 2005년 TTA에서 표준으로 제정된 상태
  - ID관리시 필요한 XML 전자서명 및 암호화 사용 가이드라인 등의 국내 표준 제정하며 이를 국제 표준에 반영하는 노력이 필요함

3.3.13. IC카드 이용 사용자 보호 기술

- 표준상태전이도 (표준화 & 기술개발 연계분석)

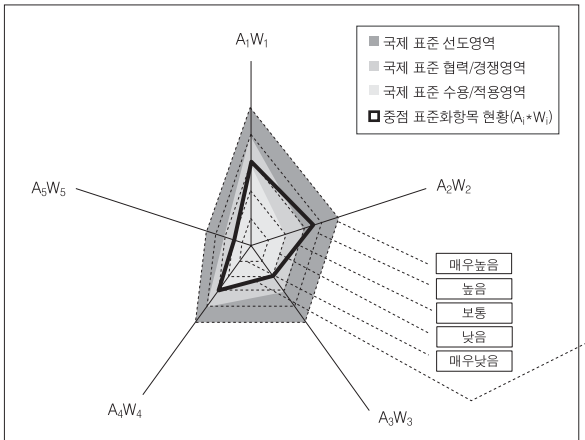


표준화 중요도	국내 개발주체		관련 국제 표준화 기구
고(★★★) 중(★★) 저(★)	표준개발	기술개발	
★★★	ECIF	ETRI	ISO

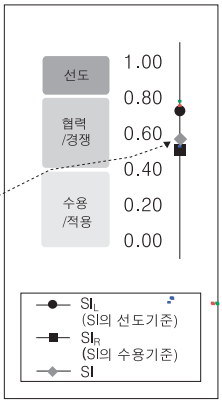
범 례

07 : 중점 표준화항목의 국내상태
07 : 중점 표준화항목의 국제상태
→ : 중점 표준화항목의 국내 표준상태전이
⇢ : 중점 표준화항목의 국제 표준상태전이
↑ : 선행표준(선 표준화 후 기술개발)
↗ : 동시표준(표준화&기술개발 동시추진)
↓ : 후행표준(선 기술개발 후 표준화)

- 국제표준화 전략목표 도출



SI (표준화 전략지수)	
SI_L (SI의 선도기준)	0.70
SI_R (SI의 수용기준)	0.50
SI	0.56



$$SI = (\sum_{i=1}^{5} A_i \cdot W_i) / 5$$
$$(0 < W_i < 1, 0 < SI \leq 1)$$

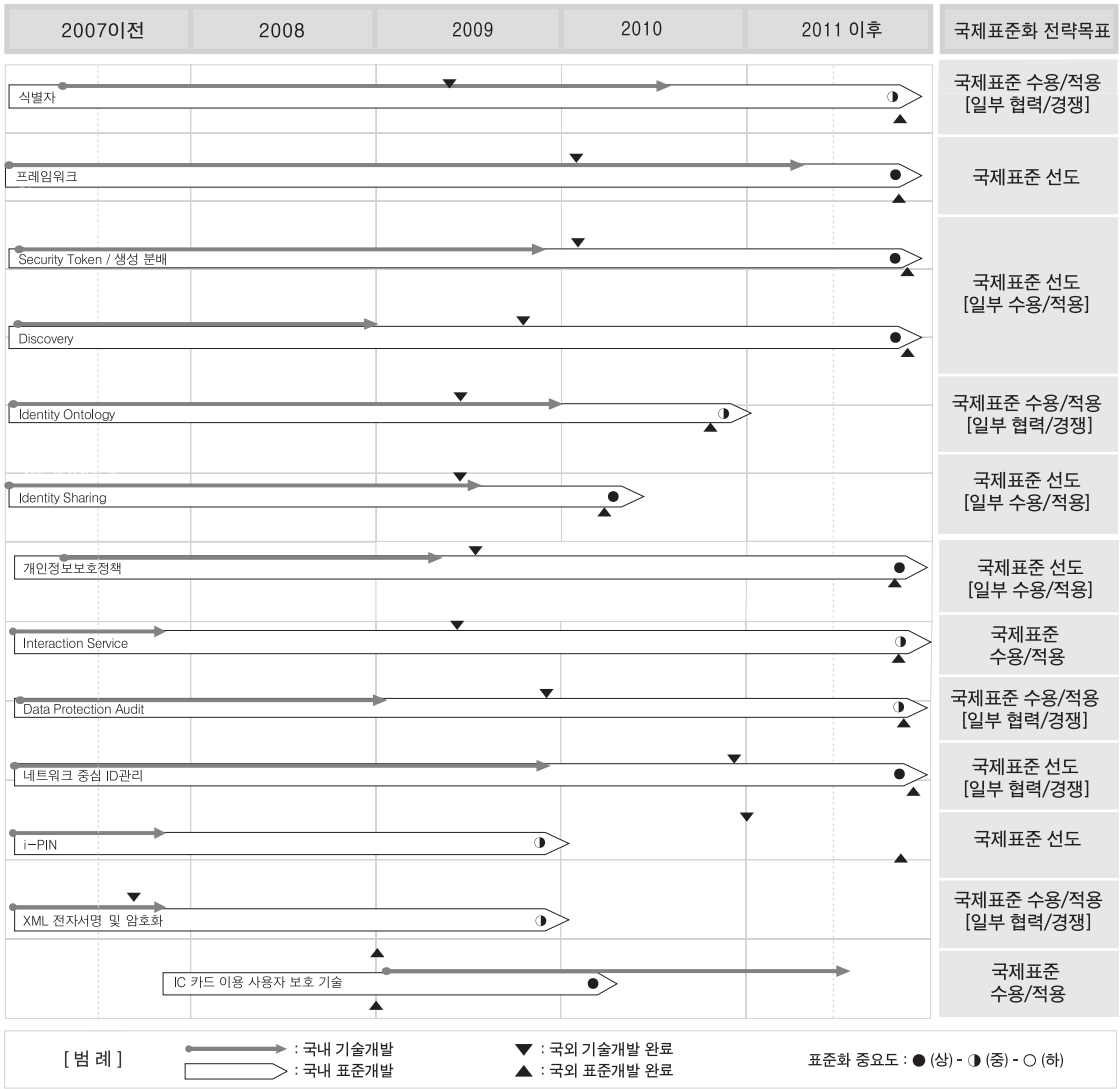
국제표준 수용/적용

- 세부전략(안)

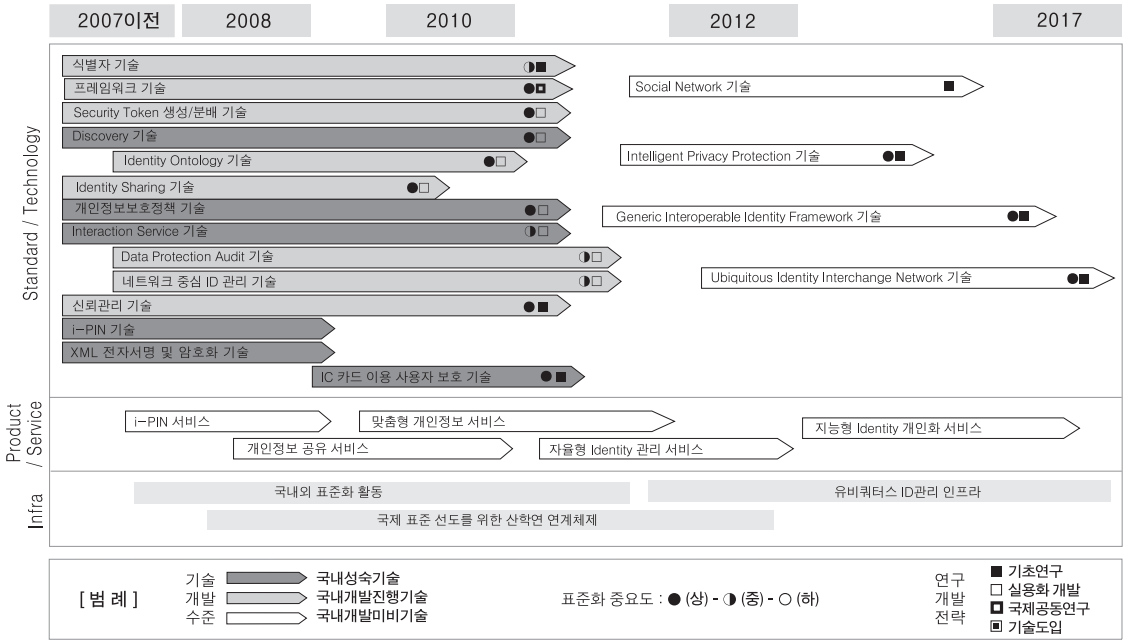
- 국제통용 전자여권은 2007년 10월 ISO 표준으로 채택될 예정이며, 이에 따라, 미국, 독일, 일본, 싱가포르, 호주 등에서 전자여권을 개발하여 일반 국민을 대상으로 발급하고 있다. 국내에서도 외교통상부에서 2008년부터 외교관 및 신청 국민을 대상으로 시험발급을 준비하고 있음
- 국제통용 전자운전면허증은 2006년에 물리규격이 ISO 표준으로 채택되어, 미국, 일본 등에서 전자운전면허증을 개발하여 일반 국민을 대상으로 발급하고 있음국내에서는 2007년부터 경찰청에서 전자운전면허증 개발을 추진하고 있음
- 행정자치부는 행정효율화를 위하여 전자주민증에 대한 개발을 추진하고 있으며, 시험 발급을 준비하고 있음
- 각 시스템을 관장하는 정부 부처에서는 일정에 따라 사업을 추진하고 있거나 추진을 준비하고 있으나, 대부분 시스템의 안전성에는 관심을 갖고 있으나 해당 ID를 소지한 개인의 정보보호에는 다소 준비가 미흡한 실정이다. 시민단체에서는 정부 주도의 정보 집중화를 우려하며, 빅브라더 논쟁을 제기하고 있음
- 따라서 향후 이용자 중심의 환경으로 전환이 예상됨에 따라, 개개인이 자신의 ID를 이용하여 권한을 보장받고 또한 불법적인 시스템의 정보 접근에 대하여 대응할 수 있는 기반을 마련하기 위한 노력이 필요

3.4. 중장기 표준화로드맵

3.4.1. 중기('08~'10) 표준화로드맵(3개년)



3.4.2. 장기 표준화로드맵(10년 기술예측)



[국 · 내외 관련표준 대응리스트]

구분	표준명	기구 (업체)	제정연도	재개정 현황	국내 관련표준	국내 추진기구
개인정보 및 ID관리	RFC 1738 Uniform Resource Locators (URL)	IETF	1994	제정	TTAS.IF-RFC1738	TTA
	RFC 3986 Uniform Resource Identifiers(URI): generic syntax	IETF	2006	제정		TTA
	Extensible Resource Identifier(XRI) Syntax V2.0	OASIS XRI TC	2005	제정		TTA
	Extensible Resource Identifier(XRI) Resolution V2.0	OASIS XRI TC	2006	제정 중		TTA
	Extensible Resource Identifier(XRI) Metadata V2.0	OASIS XRI TC	2006	제정 중		TTA
	ID-WSF(Web Service Framework) 2.0	Liberty Alliance	2005	제정 중		TTA
	X.1141, "Security Assertion Markup Language (SAML 2.0)	ITU-T	2006	제정	TTAS.IF-X1411_1 TTAS.IF-X1411_2 TTAS.IF-X1411_3	TTA
	ID-WSF Discovery Service	Liberty Alliance	2005	제정		TTA
	P3P(Platform for Privacy Preferences) 1.1	W3C	2006	제정		TTA
	P3P(Platform for Privacy Preferences) 1.0	W3C	2002	제정	TTAE.OT-10.0015	TTA
	XACML(eXtensible Access Control Markup Language) 2.0	OASIS	2005	제정		TTA
	XACML(eXtensible Access Control Markup Language) 1.0	OASIS	2003	제정	TTAS.OT-10.0040	TTA
	ID-WSF Interaction Service 2.0	Liberty Alliance	2005	제정		TTA
	i-PIN 서비스 프레임워크	TTA	2007	제정중		TTA
	i-PIN 서비스 전달 메시지 형식	TTA	2007	제정중		TTA
	XML-Signature Syntax and Processing	W3C	2002	제정	TTAS.IF-RFC3075	TTA
	XML Encryption Syntax and Processing	W3C	2002	제정	TTAS.KO-10.0185	TTA

[참고문헌]

〔01〕 A Location Privacy Protection mechanism for Smart Space, WISA 2003, 2003.08

〔02〕 A Method for Preventing the Leakage of the Personal Information on the Internet, ICACT 2006, 2006.02

〔03〕 A Technique to Protect Web Resources Using Virtual Path, CISC 2005, 2005.12.

〔04〕 An Information Security Model for the Next Generation Application Service, IWAP2002 Proceedings, 2002.10.

〔05〕 D. Hardt, OpenID Attribute Exchange, Draft Version 1.0, http://openid.net/specs/openid-attribute-exchange-1_0-07.html

〔06〕 Delegation using A Proxy Certificate in OnIDline, Systemic, Cybernetics and Informatics, 2003.7.

〔07〕 e-Authentication, http://www.cio.gov/eauthentication

〔08〕 FIDELITY project, http://www.celtic-fidelity.org/fidelity/

〔09〕 FIDIS, http://www.fidis.net

〔10〕 Global Public Key Infrastructure for Secure EIDCommerce, IWAP2002 Proceedings, 2002.10.

〔11〕 Grid ID Management based on Distributed Agents using SPML, ISCE 2006, 2006.07

〔12〕 GUIDE, http://istrg.som.surrey.ac.uk/projects/guide/

〔13〕 Higgins Project, http://www.eclipse.org/higgins/

〔14〕 Identity Management Developments at IETF-69, FG IdM DOC 147, 2007. 7.

〔15〕 Identity Management Market 2005-2009, Radicati Group, Sep 2005

〔16〕 I-names, http://inames.net/

〔17〕 ISO/IEC JTC 1/SC 27, Information technology - Security Techniques - A framework for identity management, 3rd Working Draft 24760, 2007. 6. 29

〔18〕 ITU-T FG IdM, Generic IdM Framework Requirement, FG IdM DOC 108, 2007. 7

〔19〕 ITU-T FG IdM, Identity Management in 3GPP - An Overview, 2007. 2.

〔20〕 ITU-T FG IdM, Requirements for Global Interoperable Identity Management, Draft Version 0.1, 2007 6.

〔21〕 ITU-T FG IdM, Updated Use Case Gap Analysis Report, FG IdM DOC 111R2_V7, 2007.

〔22〕 ITU-T IdM Focus Group website, http://www.ituwiki.com/index.php?title=Focus_Group_on_Identity_Management (Online; accessed 14-August-2007)

〔23〕 ITU-T Living List of Identity Management Forums, http://www.ituwiki.com/index.php?title=Living_List_of_Identity_Management_Forums (Online; accessed 14-August-2007)

〔24〕 ITU-T Living List of Identity Management Terminology, http://www.ituwiki.com/index.php?title=Living_List_of_Identity_Management_Terminology (Online; accessed 14-August-2007)

〔25〕 J. Hoyt, OpenID Simple Registration Extension, Version 1.0, http://openid.net/specs/openid-simple-registration-extension-1_0.html

〔26〕 Joaquin Miller, SXIP Specification, Version 1.0, http://yadis.org/papers/yadis-v1.0.pdf

〔27〕 Liberty Alliance http://projectliberty.org/

〔28〕 Liberty Alliance ID-SIS Specifications, Version 1.0, http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_sis_1_0_specifications

〔29〕 Liberty Alliance ID-WSF 2.0 Specifications, http://www.projectliberty.org

〔30〕 Liberty Alliance ID-WSF Data Services Template Specifications, Version 2.0, http://www.projectliberty.org,

〔31〕 Liberty Alliance ID-WSF Specifications, Version 2.0, http://www.projectliberty.org,

〔32〕 Liberty Alliance Project: About, http://www.projectliberty.org/liberty/about

〔33〕 Living List of Identity Management Terms, ITU-T FG IdM,

〔34〕 Mike Neuenschwander, Enterprise Identity Management Market 2006-2007: Not a Winner-Take-All Market, Worldwide Identity and Access Management 2007-2011 Forecast and 2006 Vender Shares, burton Group, 2006

〔35〕 Modinis-IDM, https://www.cosic.esat.kuleuven.be/modinis-idm

〔36〕 New Security Paradigm for Application Security Infrastructure, ICOIN 2003, 2003.2.

〔37〕 NIST, An Ontology of Identity Credentials Part 1: Background and Formulation, NIST SP 800-102 Draft, 2006. 10.

〔38〕 NIST, Electronic Authentication Guideline, NIST Special Publication 800-63 Version 1.0.2, 2006. 4.

〔39〕 OASIS Extensible Resource Identifier (XRI) TC , http://www.oasis-open.org/committees/xri

〔40〕 OASIS SAML(Security Assertion Markup Language) v2.0 고찰 및 응용, 한국멀티미디어학회 학회지, 2006.03

〔41〕 OASIS XRI Data Interchange(XDI) TC, http://www.oasis-open.org/committees/xdi/

〔42〕 OASIS: OASIS News, http://www.oasis-open.org/news/

〔43〕 OpenID Community, http://openid.net

〔44〕 OpenID, What is OpenID?, http://openid.net

〔45〕 Password Manager XP, http://cp-lab.com

〔46〕 Ping Identity, http://pingidentity.com

〔47〕 PRIME, https://www.prime-project.eu/

〔48〕 Reputation based public key management for mobile ad hoc network, SCI2004(The 8th World Multiconference on Systemics, Cybernetics and informatics), 2004.7.

〔49〕 Sally Hudson, Worldwide Identity and Access Management 2007-2011 Forecast and 2006 Vender Shares, IDC, 2007

〔50〕 Sampo Kellomaki, et. al, Liberty ID-SIS Personal Profile Service Specification, Version 1.1, Liberty Alliance Project, http://www.projectliberty.org/specs

〔51〕 Schema for OpenID Attribute Exchange: Attribute Types, http://www.axschema.org/types/

〔52〕 Scott Kveton, The State of OpenID, http://openid.net/pres/openid-solt-final.pdf

〔53〕 Security Assertion Markup Language (SAML) OASIS Standard specification, Version 2.0, http://www.projectliberty.org,

〔54〕 Shibboleth Project, http://shibboleth.internet2.edu/

〔55〕 Single Sign On and Access Control for network security service, SCI2004(The 8th World Multiconference on Systemics, Cybernetics and informatics), 2004.7.

〔56〕 Smart Space 상에서의 보안 요구 사항 분석, WISC 2003, 2003.9.

〔57〕 Sxipper, http://www.sxipper.com

〔58〕 Web Services Interoperability Technologies(WSIT), https://wsit.dev.java.net/

〔59〕 Windows CardSpace, http://cardspace.netfx3.com/

〔60〕 Windows Communication Foundation(WCF), http://wcf.netfx3.com

〔61〕 Worldwide Identity and Access Management 2007-2011 Forecast and 2006 Vendor Shares: IDC#207609, IDC, 2007.7

〔62〕 Worldwide Identity Theft Black Market 2006-2010 Forecast, IDC, Dec 2006

〔63〕 WS-Trust Specification, http://www.oasis-open.org/home/index.php

〔64〕 XNSORG/OneName, Extensible Name Service (XNS) Technical Specifications, Version 1.0, http://www.xns.org/pages/XNS_Technical_Specs.pdf

〔65〕 Bilinear 함수를 이용한 ID 기반 대리서명 기법, 한국정보보호학회 논문지, 2003.4.

〔66〕 Digital Identity 관리를 위한 Identity Management 기술현황과 전망, 통신소프트웨어 학술대회, 2003.7.

〔67〕 ID 기반 서비스의 표준화 동향 및 고찰, 한국정보보호학회 동계학술대회 논문지, 2004.12.

〔68〕 ID연계 기반의 인터넷ID Management System:e-IDMS, 대한전자공학회 논문지, 2006.07

〔69〕 ID중심의 분산된 UCC 관리, IUC2006, 2006.12

〔70〕 KISA 인증관리팀, Identity 관리기술 연구, KISA, 2005. 12.

〔71〕 OpenID 국내 커뮤니티, http://openid.or.kr

〔72〕 Web2.0과 URL기반의 ID관리 기술, 주간기술동향, 2006.08

〔73〕 김승현 외, "유럽의 eID 기술동향," 주간기술동향, 2006. 6

〔74〕 디지털ID현황 및 정책적 시사점, 한국정보보호진흥원, 2007, 06
〔75〕 모바일 컴퓨팅 환경에서 확장 가능한 ID 연동 시스템 설계 및 구현, 인터넷정보학회논문지, 2005.10.
〔76〕 신원도용 대응기술 동향, 주간기술동향, 2006.09
〔77〕 유럽의 eID 기술 동향, 주간기술동향, 2006.06
〔78〕 유비쿼터스 컴퓨팅과 보안요구사항 분석, 한국정보보호학회 학회지, 2004.2.
〔79〕 윤재석 외, "디지털 ID 현황 및 정책적 시사점", KISA, 2007.6
〔80〕 윤재석, 민경식, 김정희, "디지털 ID 현황 및 정책적 시사점," 정보보호 Issue Report 2007-06, 한국정보보호진흥원, 2007. 6.
〔81〕 인터넷 개인정보 유출방지 기법, ISCE2006 Proceedings, 2006.07
〔82〕 인터넷 환경에서 데이터 공유를 위한 새로운 식별체계 동향, 주간기술동향, 2006.07
〔83〕 인터넷 환경의 사용자 중심 ID관리시스템 연구동향, 한국정보과학회 학회지, 2006.12
〔84〕 인터넷 ID 관리 기술 및 표준화 동향 고찰, COMSW 2004, 2004.7.
〔85〕 인터넷 ID 관리 서비스-전자통신동향분석, ETRI 전자통신동향분석, 2005.2.
〔86〕 인터넷 Identity 관리 시스템을 위한 프라이버시 인가, 한국통신학회논문지, 2005.10.
〔87〕 인터넷 SSO를 위한 Federated Identity 기술, 2004 NCS 차세대통신소프트웨어학술대회 논문지, 2004.12.
〔88〕 인터넷서비스 환경의 고도화와 디지털ID관리기술, 주간기술동향, 2006.08
〔89〕 인터넷식별자포럼, http://www.uriforumor.kr
〔90〕 정보보호관련 법규 분석, 대한전자공학회 학회지, 2003.6.
〔91〕 정부혁신지방분권위원회, "정보시스템 구축, 운영 기술 가이드라인 버전 1.0", 정보통신부, 한국전산원, 2004.4
〔92〕 정부혁신지방분권위원회, "정보시스템 구축, 운영 기술 가이드라인 버전 2.0", 정보통신부, 한국전산원, 2005.10
〔93〕 진승헌 외, "e-Identity 보호용 공통보안서비스 플랫폼 기술 개발", 한국전자통신연구원, 2007.2
〔94〕 최준균, 이규명, "ITU-T SG13 국제표준회의 참가보고," TTA 저널, No. 111, TTA, 2007. 5.
〔95〕 편리하고 안전한 인터넷 이용을 위한 ID관리 서비스, ETRI CEOInformation, 2005.10.
〔96〕 한국소프트웨어 진흥원, 국내 계정관리 솔루션 시장 동향 및 전망, 2006
〔97〕 한국인터넷진흥원, http://www.nida.or.kr
〔98〕 한국정보보호진흥원, "i-PIN", http://www.kisa.or.kr/kisa/ipin/jsp/ipin_0000.jsp
〔99〕 행정자치부, "공공기관 통합ID 관리 시스템", http://idsp.go.kr

[약어]

3GPP	3rd Generation Partnership Project
adapID	advanced applications for electronic Identity cards in Flanders
EAM	Extranet Access Management
ENUM	E.164(Telephone) Number Mapping
FFIEC	Federal Financial Institutions Examination Council
FIDIS	Future of Identi쇼 in the Information Society
GAA	Generic Authentication Architecture
GBA	Generic Bootstrapping Architecture
GRS	Global Registry Service
GSS	Global Services Specifications
IAM	Identity and Access Management
ID-FF	IDentity Federation Framework
Id	Identifier
ID	IDentity
IdM	Identity Management
ID-SIS	IDentity Services Interface Specification
ID-WSF	IDentity Web Services Framework
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IGF	Identity Governance Framework
IMRA	Identity Management Readiness Assessment
i-PIN	Internet Personal Identification Number
IPR	Intellectual Property Rights
IRI	Internationalized Resource Identifier
IS	Interaction Service
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector
JCT	Joint Technical Committee
MOTP	Mobile One-Time Password
NGN	Next Generation Network
NIST	National Institute of Standards and Technology

OASIS	Organization for the Advancement of Structured Information Standards
OMA	Open Mobile Alliance
PRIME	Privacy and Identity Management for Europe
RBAC	Role-based Access Control
SAML	Security Assertion Markup Language
SAML	Security Assertion Markup Language
SPML	Service Provisioning Markup Language
SSO	Single Sign On
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
W3C	World Wide Web Consortium
WCF	Windows Communication Foundation
WSDM	Web Services Distributed Management
WSIT	Web Services Interoperability Technologies
WS-Security	Web Service Security
XACML	eXtensible Access Control Markup Language
XDI	XRI Data Interchange
XRI	eXtensible Resource Identifier